BUSINESS INSIDER

There is a 'game changer' technology on Wall Street and people keep confusing it with bitcoin

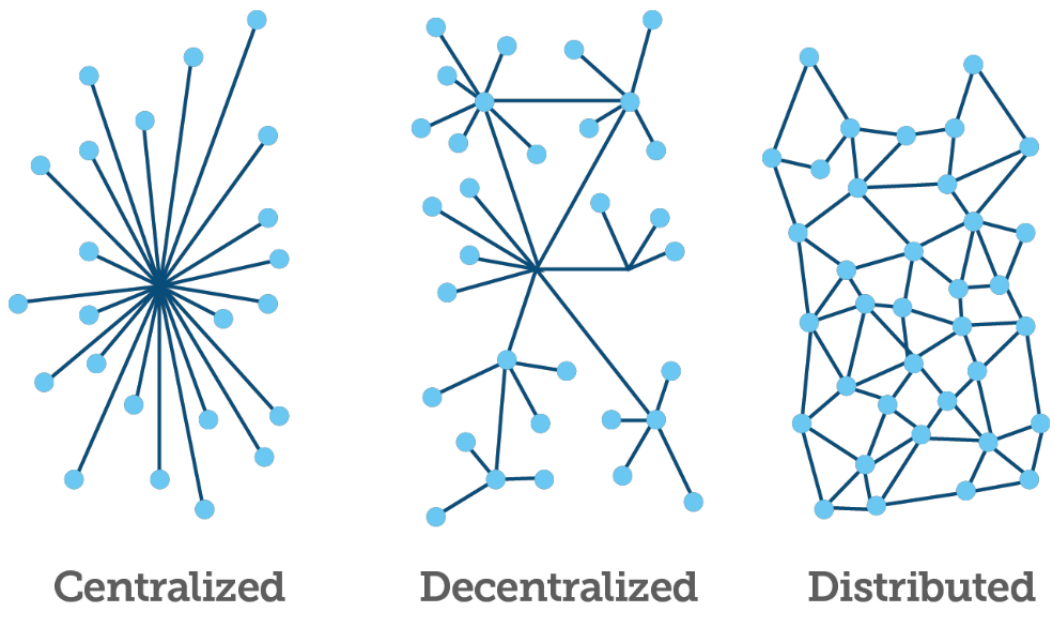
PORTIA CROWE
14H

Wall Street banks are buzzing about blockchain.

Goldman Sachs says the technology "has the potential to redefine transactions" and can change "everything."

JPMorgan last month announced it was launching a trial project with the blockchain startup led by its former executive, Blythe Masters.

Her company, Digital Asset Holdings, has secured funding from Goldman, Citi, ICAP, and a boatload of other financial firms.



Autonomous Research

Blockchains are made up of distributed ledgers.

If you're wondering what a blockchain actually is, or how its works, you're not alone. Autonomous Research, which calls the technology a "game changer," has released a report to answer all of your blockchain questions.

The important thing to understand is that it has nothing to do with bitcoin — at least for Wall Street's purposes. Blockchain is the technology *behind* bitcoin, but it has many other uses too.

Wall Street wants to use blockchains to simplify the way it processes transactions.

That may not sound very exciting, but if it works, it could eliminate back-office jobs and costs. So it's worth paying attention to — especially if you're one of the thousands of people who work in bank back offices.

Here's how it works.

Blockchains are ledgers (like Excel spreadsheets), but they accept inputs from lots of different parties. The ledger can only be changed when there is a consensus among the group. That makes them more secure, and it means there's no need for a central authority to approve transactions.

What is Blockchain?

AUTONOMOUS

A database or a ledger that maintains a continuously growing list of data records or transactions.

So, it's a spreadsheet, like Excel?

In a way yes, but it has special qualities that make it better than traditional databases.

SHARED PUBLICLY

Servers, or nodes, maintain the entries (known as blocks) and every node sees the transaction data stored in the blocks when created.

DECENTRALIZED

There is no central authority required to approve transactions and set rules.

SECURE

The database is an immutable and irreversible record. Posts to the ledger cannot be revised or tampered with – not even by the operators of the database.

TRUSTED

Distributed nature of the network requires computer servers to reach a consensus, which allows for transactions to occur between unknown parties.

AUTOMATED

The software is written so that conflicting or double transactions do not become written in the data set and transactions occur automatically.

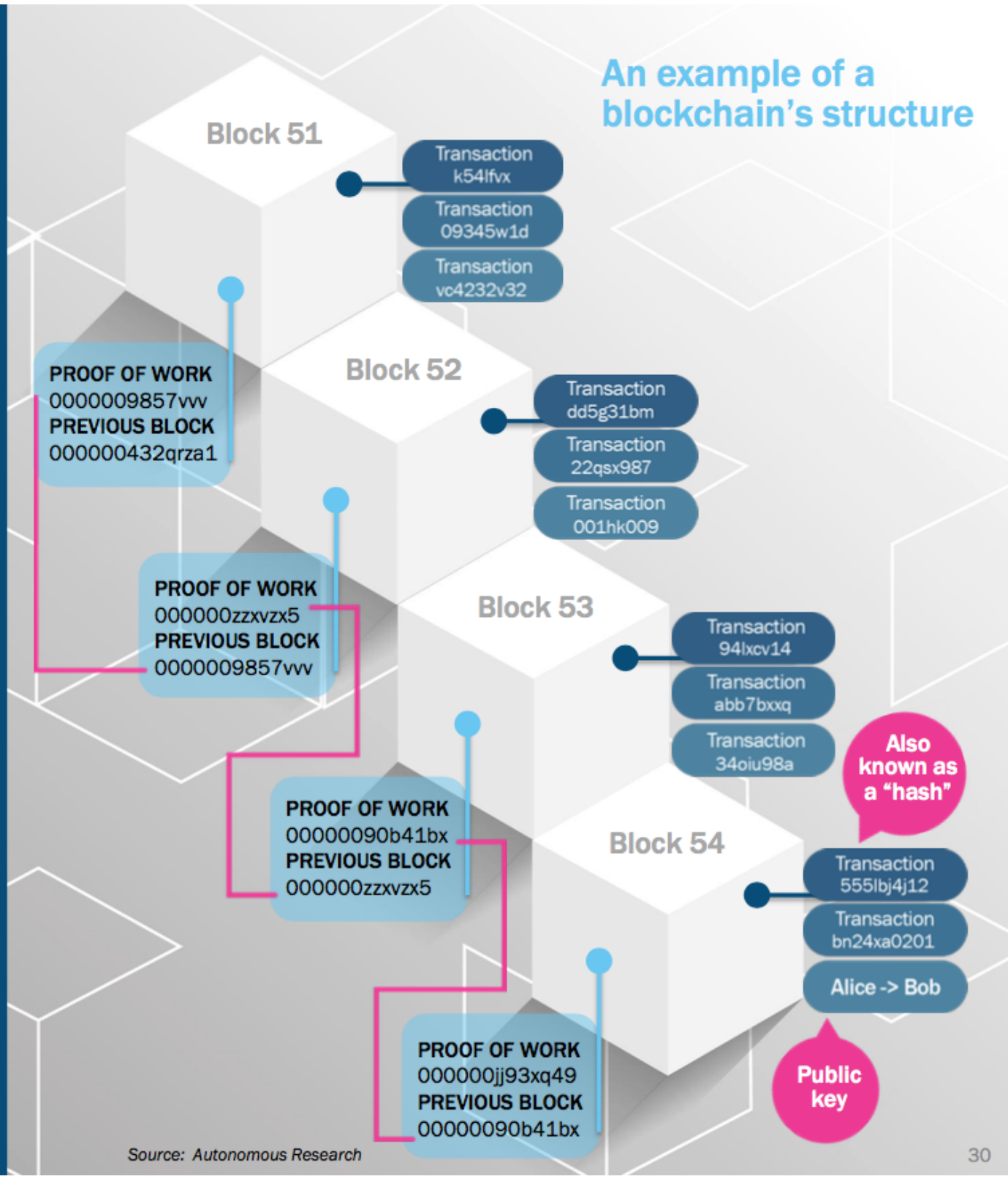
Blockchains control information and avoid duplication.

How Blockchain Transactions Work

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

There are four major pieces of information in a block:

1. An ID referred to as a "hash" or consensus identifier. In the example below, it's called "proof of work." This is a random set of encrypted numbers.
2. The hash number from the previous block, which sets the chronological order in the ledger
3. Transactions that are included in the block. Can be one, but can also be thousands of transactions.
4. Public key (identities) for the sender and receiver to identify the transfer of information.

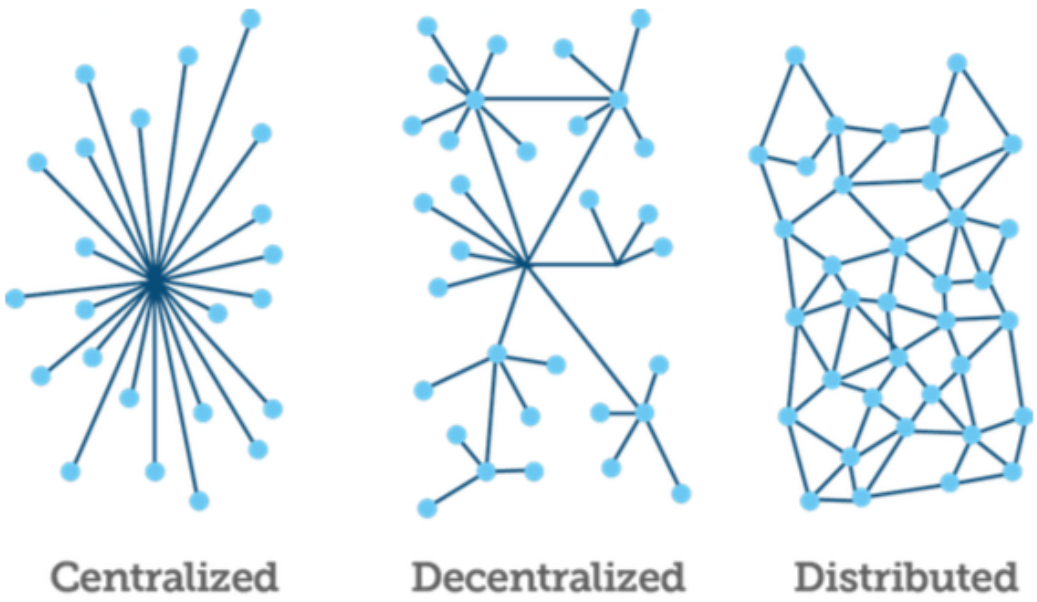


Autonomous Research

There's no need for a centralized authority to validate transactions when multiple banks, asset managers, or custodians can agree and validate them instead.

What is a Distributed Ledger?

Each block is created when multiple nodes agree and validate the transactions. This is where the term "distributed ledger" comes from as there is no need for a centralized source to validate a transaction.



AUTONOMOUS

VALIDATION OCCURS WHEN THE NODES REACH CONSENSUS. There are two major consensus mechanisms:

1. **PROOF OF WORK** – A proof-of-work (POW) protocol is an economic measure to deter ledger hacking requiring some work from the service requester, usually meaning processing time by a computer.

2. **PROOF OF STAKE** – While the proof-of-work method asks users to repeatedly run hashing algorithms to validate electronic transactions, proof-of-stake asks users to prove ownership of a certain amount of currency.

Store of value or record of value?

The ledgers do not show ownership of value but only a record of all past transactions. From these past transactions wallets can infer ownership because the record is immutable and infinitely stored.

When blockchain transactions take place, smart contracts automatically execute themselves.

Smart Contracts

Smart contracts allow for logic to be programmed on top of the blockchain transaction. When a transaction takes place, the smart contract seamlessly executes the contract. Some industry experts think that smart contracts could be the next FinTech “hype cycle”.

Cryptographer Nick Szabo coined the term ‘smart contract’ in 1994. At the time implementation was difficult because it was not easy for a computer program to trigger payments, but Bitcoin and Blockchain are changing that.

Firms such as Symbiont and T0.com (the Overstock off-shoot) have said that smart contracts will underpin securities transactions using their technologies. Smart contracts would likely be crucial to integrating blockchain architecture into the legacy systems of financial institutions.

Smart contracts could be used in real estate transactions to transfer title and release escrow when ownership is confirmed, potentially greatly reducing transaction and insurance costs. Honduras is one of the first countries experimenting with blockchain to record real estate transactions.

Peer-to-peer insurance is potentially another use-case – being pioneered by start-ups like Dynamis and Friendsurance in Germany.

Some industry participants criticize the Bitcoin blockchain’s limited capacity to handle smart contracts. Ethereum is a decentralized platform run by a Switzerland-based non-profit organization which runs smart contract applications.

What does it really mean for Wall Street? It could eliminate back-office costs — and jobs.

Cost-Cutting is the Big Hope

AUTONOMOUS

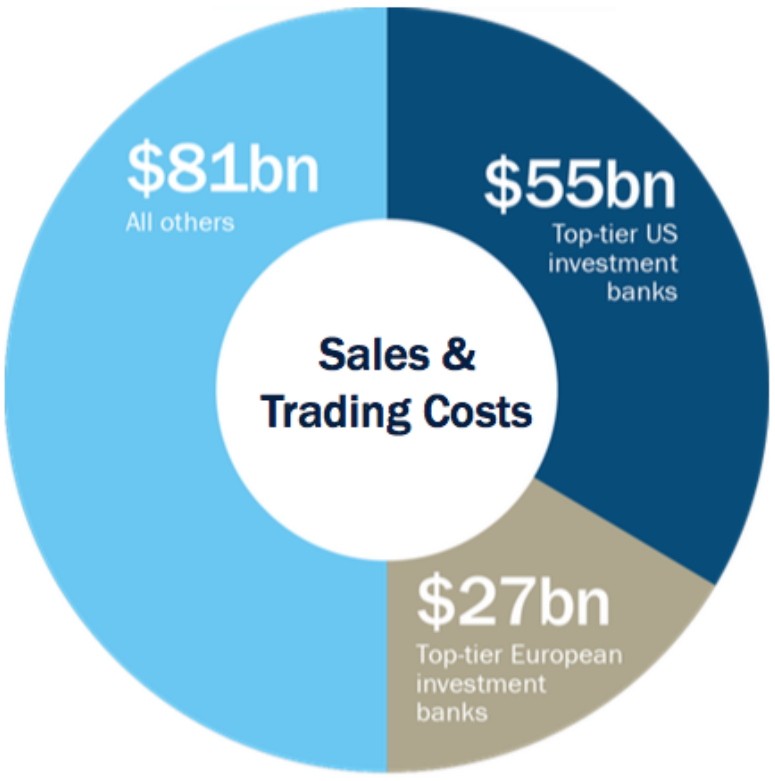
We Estimate

$54bn
annual clearing & settlement costs globally

30%
of these costs could be reduced by blockchain by 2021

$16bn
of savings for the industry

$163bn
bank sales & trading costs globally



Source: Company reports, Autonomous.

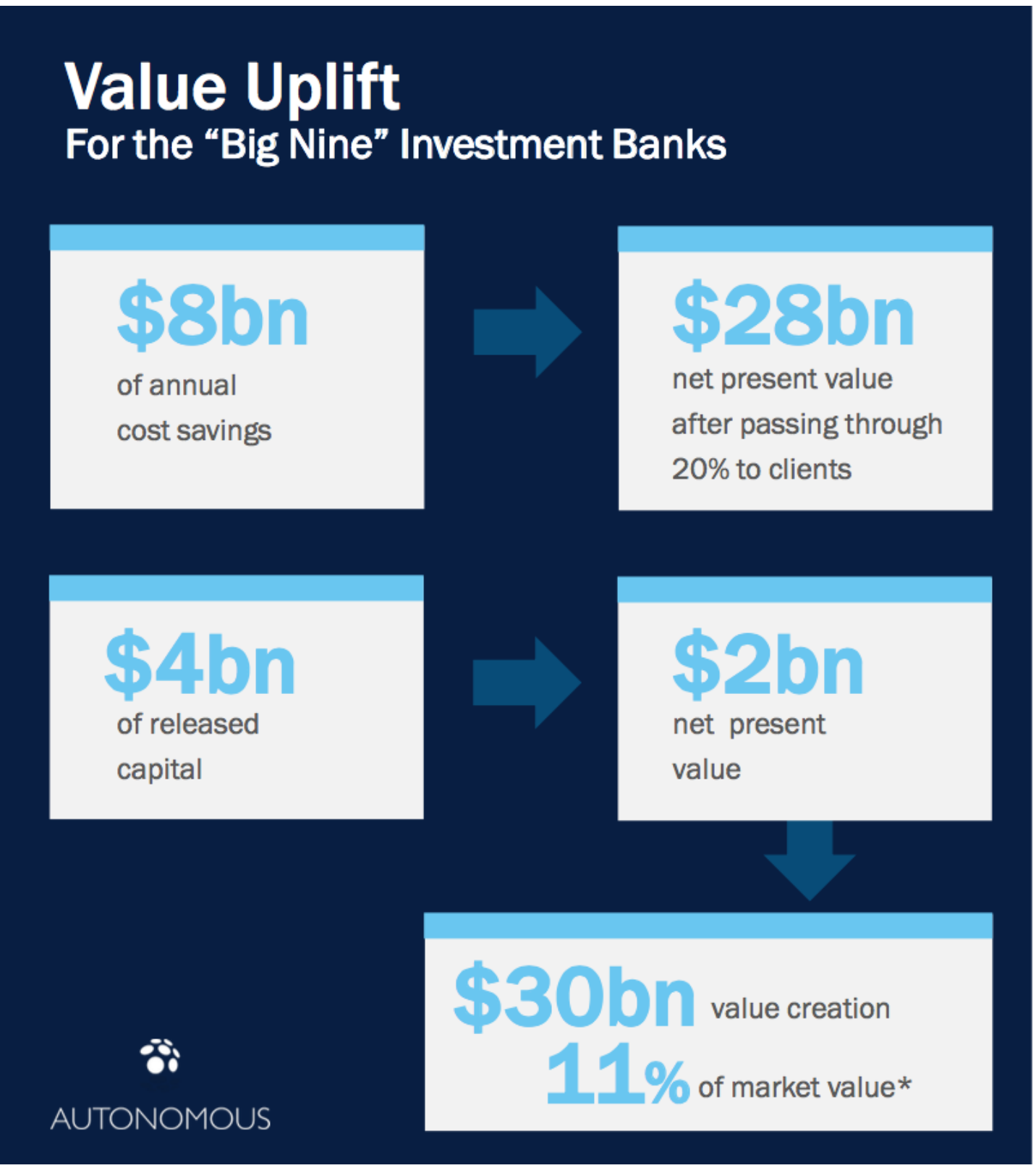
WE THINK ONE THIRD OF COSTS ARE BACK OFFICE – THAT'S $54BN. This includes costs for clearing and settlement of trades, custody, financing, books and records, reference data, reconciliations, corporate actions, tax, and regulatory reporting.

PRESSURES ON FIRMS TO CUT COSTS ARE INTENSE. If bankers don't want to cut their own compensation, then they will focus on non-staff costs, which are already elevated relative to long-term averages.

WE BELIEVE THAT BLOCKCHAIN HAS THE POTENTIAL TO BE A GAME CHANGER IN BACK-OFFICE COSTS

In our view, game changer technology should be able to cut costs by at least 20%, and more likely 30%. This suggests potential global, industry-wide savings of between $11bn and $16bn.

And it could create a huge amount of value for the top Wall Street banks. That's why they're so interested in the technology.



Goldman Sachs

Morgan Stanley

citigroup

Bank of America

JPMorganChase

Deutsche Bank

CREDIT SUISSE

BARCLAYS

UBS

Disclaimer: The use of the above listed logos is not authorized by, sponsored by, or associated with the trademark owner. The trademarks and service marks contained herein are the property of their respective owners. Any unauthorized use or disclosure is strictly prohibited.

* of investment banking divisions, as of January 2016

Autonomous Research

Here are some helpful definitions.

Blockchain Definitions

NODES – A node is a participant in the ledger. A node in the case of financial services would be a transactor like a bank, custodian, or asset manager.

CONSENSUS – The means by which all of the nodes agree on a transaction's validity. Consensus is important in ensuring the ledger's fidelity.

BITCOIN – A digital currency that is managed by a distributed ledger of the same name.

CRYPTOGRAPHY – Cryptography dates back to the beginning of written language, and is derived from the Greek words kryptós, which means "hidden" or "secret". In a blockchain cryptographic puzzles are used to verify transactions.

MINING (also called "proof of stake") – Mining is specific to the Bitcoin blockchain. Miners are computer servers that solve cryptographic problems which keep the blockchain moving forward. In Bitcoin, miners are rewarded with Bitcoin for their effort.

SMART CONTRACTS – Smart contracts allow for logic to be programmed on top of the blockchain transaction. When a transaction takes place, the smart contract seamlessly executes the contract. Examples include a derivatives contract or the additional information needed for customs in a Bill of Sale.