

Block-chain first, bitcoin later

WHY?

Because, out of the desire to create an anonymous form of payment (bitcoin), was born a potentially powerful innovation (block-chain)

Block-chain is a process to share a public common infrastructure (or **database**), yet keep all the key details (of a transaction or record) private except to the parties involved

Buzzword: distributed/de-centralized ledger

Jefferies

 **CAPITAL MARKETS**
LIMITED

 JAMAICA
OBSERVER

Television Jamaica

Just Look At Us Now!

WHY IS THIS RELEVANT?

Cost cutting and **error-reduction** (in databases)

**An intuitive example is: post-trade reconciliation
If a bank can cut trade reconciliation from days to
minutes, imagine the cost savings to the balance
sheet and capital ratios**

**Hence banks (and others) are filing patents, even
though it all started as an open technology for all**

Jefferies

 **CAPITAL MARKETS**
LIMITED

 JAMAICA
OBSERVER

Television Jamaica

Just Look At Us Now!

The “current” way	The “block-chain” way
Centralized	De-centralized/distributed
Transaction records private	Transaction records public
Encryption is localized	Encryption is EVERYTHING
Separate infrastructure / separate information	Common infrastructure / separate information
Unilateral editing rights	Only public editing rights (block-chain / bitcoin mining)

Now to what started it all: Bitcoin (in 2009)

Bitcoin is simply a **digital** (& currently anonymous) **currency** used for **transacting** OR earned as **payment** for “**block-chain / bitcoin mining**”

“**Block-chain / bitcoin mining**” is all about solving the math to verify a new block of bitcoin transactions **AND** correctly add it to **THE** block-chain (i.e. the entire chain of previous blocks of approved bitcoin transactions)

To earn new Bitcoin needs ever increasing computing power to solve the math AND the payment for correctly solving a block (of bitcoin transactions that is now irrevocably linked or the previous blocks, hence forming THE block-chain) will continue to decrease.

Effectively, **Block-chain / Bitcoin mining is currently a pyramid scheme**

So if Bitcoin is a digital (& anonymous) currency
with a **FIXED SUPPLY**.

How does this compare to fiat (i.e. paper) money?

Anything else that is money with a **FIXED SUPPLY**?

	Fiat Money	Bitcoin	Gold / Silver
Type:	Paper	Digital	Physical
Supply:	Endless	Fixed (but that could change)	Fixed
Convenience:	Easy to use	Getting easier	Getting easier
Trust:	Established	Not established	Established
Manipulation:	Very Easy	Easy - ish	Very Hard
History:	Recent	Very recent	Very long

In a nutshell,

Block-chain is:

a de-centralized / **distributed ledger** process that can **reduce costs and errors** in databases relating to transactions and records

Bitcoin is:

a digital currency **built on the original block-chain architecture.**

Fixed supply is:

the key to **prevent manipulation of money**