Blockchain Chess Analogy Summary

Imagine we are playing a game of Chess, but don't trust one another.

We write every move down, in one large book on the table. After all, we're playing for £100.

So every move is written down, with details, date and time.

Suppose I win and you're a bad and dishonest loser. You just can't help but assume you've been cheated.

You have 2 options.

First, we can replay, writing down every single move again in the book, or ledger. But you might lose.

Second, you could sneak downstairs in the middle of the night and alter the ledger. The next morning you can show the new, fake results.

That's the problem with a single, centralised ledger.

Since we don't entirely trust one another, we need an infallible way to make sure neither of us cheat.

Luckily, we're well known for our chess prowess amongst 1000s of bookkeepers. We book out the entire Wembley Stadium. 80,000 turn up. Each has their own ledger.

As we play, each bookkeeper writes into his or her ledger every move, recording the precise time to the second.

Again I win and take £100 off you.

You stew away that night and consider your options for changing the result.

You could challenge me to a second game. Replay every move and invite the bookkeepers back to re-record every move. You'd have to pay them, making that too expensive.

Or you could hire cat burglars to steal all the 80,000 bookkeepers' ledgers.

That would be virtually impossible.

Anyway the expense of doing that renders it a waste of energy and money. You'd be better off getting your own ledger and being one of those bookkeepers.

Which is how blockchain works. A blockchain holds multiple records in exactly the same time stamped way. Multiple Internet-connected computers (nodes) hold identical copies of the blockchain. When one is updated, they all update. To hack

one, you must hack all of them. It matters not if some are shutdown, as they were recently in China. They just pop-up elsewhere.

There is no human input in maintaining these records. They update automatically. Blockchains could replace centralised institutions that employ armies of people, such as banks, to check that each transaction is valid.

The only thing that is needed is transparency. The blockchain allows for that, as all records are viewable (if unchangeable).

When it comes to bitcoin, imagine 80,000 bookkeepers watching our game of chess. But on this occasion I want to pass one bitcoin to you and have that recorded so the transaction cannot be changed.

So I shout out “hey everybody, I want to send one bitcoin to David“.

Only one bookkeeper can write down the entry. To win that chance the bookkeeper must guess a number between 1 and 1 billion, like the lottery. Whichever bookkeeper does that earns the right to write the transaction into the ledger to earn a handsome reward.

That is a rather over simplified description of how bitcoin mining works. Bookkeepers who make the effort to guess the numbers are the equivalent of bitcoin miners. Their reward for mining a block (containing 3,000 bitcoin transactions) would be 6.25 bitcoin.