

Blockchains: Coercion-free consensus systems

[Nick Johnson](#)

[Follow](#)

HackerNoon.com

--

7

Listen

Share

I was recently asked what the point of blockchains was, if immutability isn't it.

I've written before about why I don't think immutability is a good term — different people take it to mean different things, and while immutability in some things is an asset (transaction records, for instance), in others it's just another term for a failure to improve and innovate.

But what is the purpose of consensus systems like blockchains? In my opinion, it's simple: blockchains provide a coercion-free way to come to consensus on something.

Blockchains are coercion free for two reasons: First, their operation is transparent, meaning anyone can inspect the current state of the system and all its past operations and verify that they follow the prescribed rules. Second, anyone who does not agree with the rules can choose to change those rules, forking off their own consensus system — what I call [pulling a Bender](#).

If a blockchain's users decide they want to make a change to the rules of the system, they can do so en-masse — such as the recent Ethereum Byzantium hard fork — but everyone must agree in order to do so. Anyone who doesn't can stick with the existing rules of the system, or propose and execute their own change. Contrary to some claims, hard forks — for whatever purpose — are not 'centralised'; they're an excellent example of decentralised governance in action. Likewise, they're not [attacks against the main chain](#); claiming they are is asserting the right to coerce people into continuing to operate under your preferred set of rules.

The ability to build a coercion-free system is pretty unique. In the real world, people cannot simply fork the world to suit their needs. Catalonia cannot 'fork' Spain to achieve independence, because the resources involved are shared and cannot be duplicated.

Different design decisions can make this property weaker or stronger. Robust replay protection makes pulling a Bender less risky. The Ethereum Ice Age discourages stasis, while still providing for other forms of disagreement to be expressed by rule changes and forking.

Critics will point out that forking may not achieve everything those involved want it to: the other fork may retain the ticker, or gain applications and adoption that their desired fork does not. This is just the flip side of the same freedom: just as nobody can coerce you to play by their rules, you cannot force anyone to play by yours. You are entitled to have your own theme park, but you can't make anybody come use it if they don't want to.

Incidentally, proof of stake will ultimately make forking simpler, by eliminating the spectre of 51% attacks against forked chains. I anticipate more forks over smaller differences once more chains use Proof of Stake. Hopefully the 'healing factor' of better inter-chain interoperability will make this less of a problem for those wanting to build applications with wide adoption.