Holochain Consistency vs. Global Consensus

Perry Kundert

2019-09-17 23:00:00

Can Global Consensus cryptocurrencies be used as money? PDF/Text

Bitcoin, Ethereum, etc. have completely different implementations, but share a common idea – that **all** transactions in their ledgers are agreed to by all participants, simultaneously; that there is a single, agreed-upon global "state" of the ledger's data at each point in time.

This data-centric, distributed global synchronous, simultaneous agreement amongst **all** blockchain participants differs greatly from how money currently works, and brings with it a number of surprising results. When properly understood, it is unlikely that these systems could ever be widely accepted as a form of money.

Recently discovered agent-centric blockchain algorithms provide strong guarantees about the global ledger, but relax the unnecessary synchronous, simultaneous agreement requirement. This allows for correct operation even in the face of network partitions, delays and failures, and performance that scales linearly with the number of participants (eg. to millions of operations per second) – even if participants are separated by large network delays.

Contents

1 Money Just Has to Work **2**
- 1.1 CAP: What Happens When Disaster Strikes 2
- 1.2 Could Such a Network Partition Disaster Happen? 5

2 Simplicity, Safety and Security **5**
- 2.1 Public/Private Keys 5
- 2.2 Hardware Wallets 6
- 2.3 What You Know + What You Have 6
- 2.4 Revoking Your Way to Security 6

3 Summary **7**

1 Money Just Has to Work

Money that won't buy things isn't just inconvenient; it is dangerous. Cryptocurrency based money, especially those based on Global Consensus systems (basically, all of them) are especially fragile. Only during globally calm, disaster-free idyllic periods of history could they possibly pass as useful money.

Money must have, at the very least, a few few commonly acknowledged features that roughly break down into 3 categories **Consistency**, **Availability** and **Partition-tolerance**, or **CAP**:

- Consistent: it's not easily counterfeitable, and balances are verifiable
  - Valuation vs. common assets
  - Divisibility
- Available: you can always buy/sell something for cash money
  - Common and accessible
  - Constant utility
  - Low cost of preservation
  - High market value in relation to volume and weight
- Partition-tolerant: if you can "talk" to someone, you can do a deal
  - Resistance to counterfeiting
  - Recognisability
  - Transportability

If your money fails to have one of these groups of features, it can still have utility – but you must accept the consequences! Some of these consequences are likely to be **extremely** surprising to owners of Bitcoin...

1.1 CAP: What Happens When Disaster Strikes

The CAP theorem claims, basically: Consistency, Availability or Partition-tolerance – pick any two. It is not possible to have all three in the case of a Partition. But, ideal money is widely assumed to have all three **CAP** features!

Let's survey some of the combinations of **CAP** that you might recognize from real-world systems, and see what they would do in certain failure scenarios.

1.1.1 AP: Bitcoin

Global consensus cryptocurrency systems are sometimes AP; they give up Consistency to maintain Availability, in the face of a network Partition. Bitcoin will carry on processing transactions and mining new Bitcoins inside each partition of the network. When the partition ends, all but the longest chain will simply disappear. It will maintain "Availability" to all participants, inside every separate "Partitioned" network, through the duration of the network event.

This is, obviously, *false* Availability. Bitcoin will process transactions and mine new Bitcoins inside each Partition of the network – but when the Partition ends, all but the longest chain simply ... **disappears**! All ledger balances adjusted in all the Partitions of the network containing "shorter" chains vanish.

For those in the "disappeared" fork, was the system *really* available? No, it was not – all of their transactions ceased to exist. The remaining Bitcoin blockchain is "Consistent", all right – consistently absent of all of their transactions.

That something; just not ... money.

From the perspective of the spenders and recipients of Bitcoin transactions within the affected network Partitions; it would be as if they received "counterfeit" Bitcoin. It seemed to be "recognizable" as Bitcoin (at the time of the transaction). It seemed to be "transportable" at the time, but clearly was not.

So, Bitcoin has great utility and high network-effect due to its great age and wide-spread recognizability. But at best it should be considered an "asset", not "money".

1.1.2 CP: Hashgraph, "ACID" Databases

Hashgraph (hBar, Carbon, and perhaps some other cryptocurrencies) will stop, in whatever part(s) of the network cease to have a majority quorum of signatory nodes, and then resume when the partition re-joins the larger network.

So that's at least better; we can't "seem like" we're doing an hBar cryptocurrency deal, and then find out later that it just blinked out of existence.

At least it works at tens of thousands of transactions per second, with absolute settlement in seconds, when it works! But, what do I do about food when I happen to be disconnected from the 'net for a couple of weeks?

Better; still just not quite ... money.

Availability is simply not an optional feature for "money". It means real-world inconvenience at best, starvation at worst.

1.1.3 CaP: Holofuel

Holo's Holochain based systems maintain Consistency, giving partial Availability in the face of a Partition. The HoloFuel cryptocurrency used by Holo for hosting payments, etc., is an example of what is possible, beyond the restrictions of global consensus systems.

You can transact a deal with any other party that you can communicate with (of course, you can't deal with other agents you can't communicate with, which sort of makes sense).

Furthermore, the deal is validated by as many nodes are available within your partition. Of course, don't do a billion-dollar deal if you're in a mobster's network and can only see a few of his nodes. But, even if you do – as soon as you rejoin the larger network, any attempt at fraud will be *immediately* discovered. Unlike statistical consensus, which agrees with a majority (the 51% attack) – it only takes a *single* non-fraudulent node to detect and report fraud, and then any and all other nodes can confirm it, and black-list the complicit parties.

Worst case – *if* you decide to accept the high-risk transaction – you'll have to Decline the (unfortunately fake) funds you were paid, to restore your account to non-fraudulent status. But, for most typically use cases, the cost of building the fantastically complex and elaborate "charade" required to perpetrate a *single* fraudulent transaction won't be worth it. Especially since the ill-gotten funds will immediately become *worthless* – nobody will deal with the account – as soon as the fraud is detected by a single other node!

In Holofuel, it is trivial to avoid even the possibility of this happening; simply include one other trustworthy Holofuel Agent in the transaction, whom you *know* is outside the hostile network you are within; your partner's Holofuel account, for example. These can be zero-value participants, who only need to sign the transaction, but don't contribute or receive any part of the ledger balance transfer.

These risks and mitigations are somewhat analogous to cash:

- Don't take suitcases of "totally legit!" USD$100 bills from a North Korean stranger in exchange for your yacht.
- Don't trust a certified cheque from "Bubba's Bank and Trust and Taco Shack", or from the "Royale Bank of Scottland" branch in the City of

Culiacán, Sinaloa, Mexico.

That's more like money!

1.2 Could Such a Network Partition Disaster Happen?

Communication across oceans is *not* as simple and reliable as our experience over the last 70 years would imply. We live in an idyllic, peaceful period that is not representative of the bulk of human existence.

Can you reasonably assume that every major global superpower is *so* incompetent that they do not know the location of each and every one of their enemies' sub-sea fiber cables? If each sub-sea cable is *not* equipped with explosives by **more** than one opponent, I would be utterly shocked.

Such a situation (if it occurred) would be a *complete* failure of *every* modern military power to plan to achieve one of the most basic rules of battle – to deny your opponent access to the field of battle on their own terms. Controlling the flow of information is one of the basic requirements for modern battlefield control. You can therefore be completely assured that (at least) China, Russia and America have complete control over the health of their opponents' global communication trunks.

Within the first few minutes of the next global "kinetic" power confrontation, the "pop! pop! pop!" you hear will be the destruction of your global internet connectivity. Good-bye, Global Consensus!

And, Good-bye Bitcoin!

2 Simplicity, Safety and Security

If you can't explain how money works to a drunk guy at a bar, or teach your dad how to use it – it's also not money.

When you make one small mistake, and it all disappears; well, while that's sort of like money, it's not ideal. Money stored in an account must offer layers of protection that prevent a single error from emptying the account.

2.1 Public/Private Keys

The majority of cryptocurrencies use some form of public/private key pairs to identify accounts (the public key), and authorize transactions (the private key).

For Bitcoin, Ethereum, and most others, what this means is: if you ever reveal your private key: you're toast. Your account balance is gone, the instant that someone ever discovers that private key.

It might happen now, in a month or 3 years from now – but once your private key is left open (sitting on a desk, in an unencrypted file on your computer, in a filing cabinet, buried in your back yard, ...) – your balance will simply blink out of existence, into someone else's account. You'll totally be able to see exactly where it went; but you can never, ever recover it. It's gone.

2.2 Hardware Wallets

The Hardware Wallet seems to a solution. You can't leak your private key, because you can never "get" it; you ask the hardware to sign stuff, and it never gives up the key. Some good options are the Trezor Safe or the Ledger Nano.

You still have to save the root entropy seed (those pesky 12 or 24 BIP39 words). If anyone ever gets them, they have not just your one leaked wallet's contents – they have them all. So, not really a perfect improvement (however, you *can* securely and reliably backup and recover your BIP39 Mnemonic using SLIP39).

2.3 What You Know + What You Have

2FA (2-Factor Authentication) is an improvement.

In Holo's HoloFuel, to make a transaction, not only do you need the signing private key; you also must prove that you hold certain data from private source-chain entries, which have never left your devices. They aren't printed anywhere (they are backed up, using passphrases unrelated to your private key, between all of your devices). They are entirely independently secured.

So, an attacker must A) get your private key, and B) get your device (or its backup from another of your devices, plus discover the backup passphrase).

Compared to typical cryptocurrency wallets, stealing funds requires both collecting key data, plus physically or logically penetrating a physical device that is in your possession.

A *much* higher bar; more like real money.

2.4 Revoking Your Way to Security

Everyone makes mistakes. Requiring you to destroy all of your accounts and create new ones every time you *may* have possibly made a security mistake

is not great, but that's the best we can do with public/private keys and plain 2FA.

Using Holo's DPKI (DeepKey), you can revoke and reissue your private keys at any time. You retain your account's ID (its original Public Key), so all of your account relationships remain intact – but a new Private Key is required for all future transactions. To accomplish this, you need a "revocation key" issued for the account, which you would do at account creation.

These revocation keys can be generated and stored in N fragments with multiple trusted parties; spouse, lawyer, accountant, family friends, bank safe-deposit boxes, filing cabinets, etc. When required, they can be reconstructed by collecting M of N of these fragments, where M <= N.

Very much like money, stored in a safe that can only be opened with the collaboration of the majority of your most trusted third-parties.

3 Summary

The day is coming when the creation of money will be wrested from the hands of central authorities and placed back into the hands of individual wealth creators. In the mean time, at least we can now offer money substitutes that allow free people to convert their debasable Fiat money into a more value-stable, safe, efficient and useful form.