Synchronising Life & Dreams.

Why blockchain is not yet main stream?

May 2018 · 6 minute read

The current state

There is a lot of hype about what the global distributed ledger aka “Blockchain” can do for society. A “trust machine” as some people call it that will bring the power of finance, data sovereignty and inclusion to the people, hence rendering centralized intermediaries like Visa, Barclays & Facebook obsolete.

We shall achieve this by using a combination of robust, battle tested cryptography & game theory.

While this vision is plausible, realizing it is not a easy as it may seem.

The blockchain is not yet ready.

The core barriers to mainstream adoption

The blockchain, while being a new concept in decentralized distributed databases has also presented very unique set of problems in computer science & economics that have never been solved at the time of this writing.

Is this post, I will talk about the the 6 most important issues only with which if solved, shall we (blockchain enthusiasts) ever achieve our vision.

1. Scalability Issues.

The current bandwidth, i.e the data that can be transmitted through a blockchain with in a given time is simply too bounded for main stream adoption.

Ethereum for instance does a maximum of 13 transactions per second. Visa on the other hand can do 24,000 Transaction per second and peak over 40,000 transactions per second.

So as you can see, the blockchain is thousands of magnitudes unable to manage a global traffic of financial transactions. This is what they call the “Scalability Problem”

Coming up with a solution to scalability the problems without tarnishing the original value propositions of a blockchain (immutability/security, decentralisation & censorship resistance) is not trivial. It has been nick named the “scalability trilemma” by Vitalik (Ethereum’s co-author).

2. Lack of Intuitive Private Key Management.

Ordinary users will simply never wrap their heads around private keys.

Private keys, which are a string of text used to sign transactions and make other proofs(cryptographic).

The purpose for these proofs or signatures is for other entities on a blockchain network to verify identities & messages amongst themselves without reasonable doubt.

Private keys have two main problems first, how to store them securely.

Anyone who can memorise, take a picture, or copy your private key can literally steal all your money. Because they have your private key, they can make the cryptographic proofs/signatures and *accurately prove to everyone on the network they are you* even without your consent. Even when they are not you.

Second, you loose your key you loose access to all your money & *no one can ever help you out*. There is no “click here to remember your private key”

We need to first come up with something as intuitive using ATM/Debit cards.

Imagine if your bank told you that, “if you forgot your Debit card PIN, you loose access to all your money with *zero hope of recovering it how ever large a sum of money it would be*”.

If the above was the case, I dont think any one would use debit cards. For the reason, find it fair to call people that keep significant amounts of cryptocurrency with under a private key *Ultra risk takers*.

3. Contract unsafety.

It is simply not reliable & safe for responsible institutions & individuals to deploy smart contracts on blockchains like Ethereum.

Due to the blockchains having an immutable and unpredictable state. Smart contracts deployed on such a platform are also expected to suffer from immutable bugs & unpredictable events.

As a result, millions of dollars have been lost in events such as the theft of $50 million from TheDAO and Parity’s $160 Million loss of funds

I was glad that Rick dudley talked about this

4. Consensus algorithms are wack.

The popular blockchains only don't offer transaction finality i.e you will never be 100% sure that you have gotten funds.

You can only be probabilistically to a high degree (but with zero guarantee) that you have received your funds. This is because in major consensus algorithm called Nakamoto Consensus, the miners elect the longest chain with the most computational work that are with in the same protocol i.e consensus rules.

For instance imagine your bank tells you that you that, "there is a 95% chance that we *might* have your life savings, however you may also not poses it in 5 years in case we discovered that the longest chain with the most work does not have your transaction in it"

Yes, I dont think anyone wants to keep their life savings in such a bank.

5. Privacy.

Just by knowing someone's cryptocurrency address, you can know their account balance & transaction history simply by pasting it in a blockchain explorer like blockchain and etherscan

Meaning its very easy for anyone to keep track of your financial activities without permission.

You buy HIV drugs? I now know your HIV positive, Your paying schools fees? now your local kidnapper knows where your kids study. No careful person wants that!

6. Price volatility.

Very few people simply don't have the stomach to hold a financial instrument that drops by over %50 with in a few months.

What are People are doing?

There are majorly two things that go on in the blockchains industry, a) Building of blockchain solutions, and b) Speculation/Investing

a) Building

Most projects are building on platforms that have these problems regardless in hopes that they will integrate solutions to the issues in the future.

The risk they face however is that the platform they built on my become obsolete after a heavy investment of time & resources on the wrong platform.

Think how the micro payments industry died in bitcoin because of high fees

It's like building your phone app around a windows smart phone only to be made irrelevant because the next generation of your will not be using windows smart phones, but iOS and Android.

b) Solving

A number of projects are working on the issues above.

For instance;

Scalability: Rchain Doing work on sharding, HashGraph using the gossip protocol to achieve finality and consensus in permission systems.

Key Management: Ledger using Hierarchal Key Derivation to store private keys in a secure easy manner. i.e easy to read & store 24 english words found in literature.

Contract safety: Zilliqa with their automata based programming language called, scilla that employ's formal verification using Coq. That will allow contracts to run safely & predictably.

Consensus Algorithms: Algorand using what they call a "rapid and efficient user consensus, enabling even the smallest transactions, regardless of transaction volume or number of users" to achieve transaction finality.

Privacy: Zcash, Zcoin & Monero using Zero knowledge proofs and Ring signatures respectively to achieve privacy benefits.

Price Volatility: Digix's DGD tokenising gold tokens to offer protection from volatility, Dai's Maker DAO & Basis intend to create cryptocurrency with stable prices completely maintained by digital resources.

Fell free to send comments on twitter thread