Blockchain: Expectations & Reality

Ali Aydın Selçuk
TOBB-ETÜ

Blockchain: Great Expectations

- Most talked about technology of recent years.

- "[Blockchain] is the biggest opportunity set we can think of over the next decade."
  – Bob Greifeld, (former) NASDAQ CEO
- "We'll all look back in 20 years and conclude that Bitcoin was as influential a platform for innovation as the Internet itself was."
  – Marc Andreessen, WWW pioneer, investor

Blockchain: Great Expectations

- "Bitcoin is the most important invention in the history of the world since the Internet."
  – Roger Ver, Bitcoin investor and evangelist
- "Virtual currencies may hold long-term promise, particularly if the innovations promote a faster, more secure, and more efficient payment system."
  – Ben Bernanke, (former) Fed chairman
- "The blockchain cannot be described just as a revolution. It is a tsunami-like phenomenon."
  – William Mougayar, author

So, What is Blockchain?

- At its core, it is a distributed ledger, shared over a P2P network.
- Everybody keeps a copy of the public ledger, and transactions are recorded in the ledger regularly.
- But if there is a conflict between user copies, no authority exists to resolve it.
- Instead, consistency is maintained by a "consensus algorithm".
- New records are added to the ledger in "blocks" (~pages) after some sort of consensus.

Consensus Algorithms

- The most interesting feature of the blockchain technology.
- Many alternatives exist: PoW, PoS, BFT, …

- Proof of Work (PoW)
  - System deliberately slows down the block addition process.
  - A puzzle has to be solved to add a new block.
  - For consensus, any ties are broken by extra effort.
  - Side effect: enormous waste of resources

Consensus Algorithms

- Proof of Stake (PoS)
  - Miners invest their holdings in the mining process.
  - It can be used in conjunction with PoW.
  - It saves resources that would be wasted in PoW.
- Byzantine Fault Tolerance (BFT)
  - A small, select group of users communicate and approve a new block.
  - Very efficient
  - Q: Which users will be in the consensus group?

Promises of Blockchain

- Distributed public ledger
- Digitalized data
- Updated near real time
- Chronological & timestamped
- Cryptographically sealed
- Irreversible & auditable
- Operates without any trusted authority

- A trusted system without a trusted authority! (utopia of a crypto-anarchist)

Sectors Expected to Benefit

- Financial transactions
- Supply chain management
- Healthcare management
- Verification of credentials (license, diploma)
- Digital voting
- …

The Hype

- After Bitcoin's sensational success, the blockchain was seen as "the next big thing".
- There was certainly a hype:
  - Long Island Ice Tea changed its name to Long Blockchain Corp. and its stock jumped from $2.44 to $6.91 in December 2017.
  - Kodak announced KODAKCoin, a photo-centric cryptocurrency for image rights management, and its stock jumped from $3.10 to $9.20 in January 2018 (which is down to ~$2.40 in October 2018).

The Hype

- Lot of investment capital was poured into blockchain projects, causing even more hype.
- “Blockchain” was coupled with almost anything, meaningful or not.
- Reminiscent of the dot-com hype of the late 1990s.
- People have been looking for the great “killer applications” of blockchain.

Doubts

- Bitcoin has been around for ten years, Ethereum for five. Blockchain potentials have been talked about for long.
- Still nothing like the promised killer apps has emerged.
- Blockchain risks looking like a solution in search of a problem.
- Unlike thought, people don’t dislike authority and demand truly decentralized systems.

A More Critical Look

- We need to question our assumptions about a desired solution.
- Many real-life problems don't need a decentralized solution and are better served by a client-server architecture.
- Actually, a trusted authority is something preferable for most people in case of a dispute.
- In reality, the libertarian or anarchist view is a small minority in society.

A More Critical Look

- Many perceived advantages of a blockchain system come from added functionalities, such as,
  - digitalized data
  - regular data entry
  - PKI
  - online service

- With similar assumptions, a client-server solution can just be built and operated more easily and cheaply.

Example: Supply Chain

- Walmart recently announced a system to track its vegetables, using blockchain.
- Produces will be traced all the way back to the farm, for food safety.
- In fact, Walmart started a similar program in 2006, and then abandoned it in 2009 due to problems with getting everyone to enter data.
- So, why a blockchain instead of a server?

Example: Driver's License

- State of Florida announced a plan to keep digital driver's licenses on a blockchain.
- So, police officers will be able to access the record online, from anywhere.
- But what does blockchain have to do with all this?

Example: Academics

- Universities will keep student credentials (transcript, diploma, etc.) on a blockchain so it can be accessed online.
- A server by the university or a public entity would be easier, but blockchain has its advantages.
- Advantages of blockchain:
  - An online, integrated database of credentials.
  - Credentials will be accessible even after the university is closed permanently. (?)
  - Proof against abuse by the university. (?)

Example: Settling Roaming Charges

- In GSM roaming, the visited operator (VPMN) presents usage records to the home operator (HPMN) for payment.
- Their records may differ and they need to settle.
- Blockchain solution: instant settlement!
- Not exactly: They can't agree on the data to be entered in the first place.

Example: Election Security

- Results of elections can be controversial (e.g., USA 2000).
- Blockchain provides a way for tamperproof record keeping.
- Well, in case of election fraud, data is tampered with *before* it is recorded.

Example: Smart Contracts

- Smart contract: “Code is law.”
- A contract is encoded in a programming lang. and stored in the blockchain.
- When some condition is met, payment is made in the blockchain, possibly triggered by an “oracle”.
- Oracles communicate real-world events (location, temperature, or some online event) to the blockchain, in a trusted way.

Example: Smart Contracts

- Smart contracts, for now, are not legally-binding contracts as we understand it.
- Legal regulations don't seem near nor easy.
- Just recall all the regulations required for the qualified electronic signature law.
- For the foreseeable future: "Code is law."

A More Critical Look (recap)

- We need to question our assumptions about a desired solution.
- Many real-life problems don't need a decentralized solution and are better served by a client-server architecture.
- Actually, a trusted authority is something preferable for most people in case of a dispute.
- In reality, the libertarian or anarchist view is a small minority in society.

A More Critical Look (recap)

- Many perceived advantages of a blockchain system come from added functionalities, such as,
  - digitalized data
  - regular data entry
  - PKI
  - online service

- With similar assumptions, a client-server solution can just be built and operated more easily and cheaply.

Sceptic's View

- As the hype became obvious, skeptical viewpoints have been more widely expressed.
  - "The only reasonable use case for blockchain is electronic money." (J. Song)
  - "Blockchain is a useless technology." (N. Roubini)

- I don't agree. Middle ground is possible.

Balanced View

- Blockchain,
  - is not a useless technology,
  - nor is it the next big thing after the Internet.
- Blockchain is a good invention with neat features.
- But demand for a truly decentralized system is not high in practice.

Reasonable Use Cases

- In many cases, blockchain is seen as a way of integrating databases of different entities for online service.
- These applications make more sense when no trusted authority exists. For instance,
  - healthcare database in the US vs. Turkey
  - diploma database in the US vs. Turkey
- If an authority exists, a similar functionality can be achieved by a server much more easily.
- Similarly, international use cases are usually more meaningful than national ones.

Reasonable Use Cases

- International money transfer
  - Blockchain systems like Ripple & Stellar are real alternatives to SWIFT, MoneyGram, Western Union.
- International environmental protection
  - Sensors will enter data to a public database without any censorship.
- Pharmaceuticals: drug supply chain
  - Drug Supply Chain Security Act of 2013
  - Drug companies and partners are to more closely track where their finished products are shipped.
  - A decentralized database may help.

Outlook on Cryptocurrencies

- This is a whole different story.
- Recall what Bernanke said:
  "Virtual currencies may hold long-term promise, particularly if the innovations promote a faster, more secure, and more efficient payment system."
- It may very well be the next big thing in the history of money.

Outlook on Cryptocurrencies

Brief history of money:

- barter
- commodity money (salt, cattle)
- precious metals (gold, silver)
- paper money
- electronic payment
- cryptocurrencies (?)

Maybe. Hard to tell. People were skeptical when paper money displaced gold. Coming generations will decide.

Obstacles to Blockchain Adoption

After so many years of hard work, so much investment, and so many proposals, why don't we see any common usage of blockchain?

- No sense of urgent need
  - Even if blockchain has pluses, a client-server solution is 99% satisfactory for most cases.
- Lack of understanding and trust
  - Security features of blockchain is hard to grasp even for computer scientists.
- Doubts on cybersecurity
  - Theft in 2018: ~1 billion USD.
- Lack of legal regulations

Beyond the Hype

- Blockchain is not just a hype. It is a real invention with neat features,
  - decentralized public ledger,
  - tamperproof & auditable.
- But proposed applications must be scrutinized:
  - Is there a need for a decentralized solution?
  - Against what kind of risks are we defending?
  - With the same assumptions (digitalized data, PKI), how would a client-server solution do?
- Cases with satisfactory answers will have a potential for use.

Conclusions

- Blockchain is a novel technology.
- But it has been the subject of a huge hype for the past couple of years.
- Things will normalize and we will see the real uses of blockchain.
- Recall the dot-com bubble of the 90s:
  - The bubble bursted and 99% of the companies disappeared.
  - But the remaining few like Amazon and Google did indeed change the world.
- Will history repeat itself?