Day 1 Assignment

Advance Blockchain

Summary of Bitcoin white paper published by Satoshi Nakamoto:

Ten years ago, on October 31, 2008 an unknown person or entity called Satoshi Nakamoto published the revolutionary whitepaper "Bitcoin: A Peer-to-Peer Electronic Cash System" which birthed a $200 billion crypto industry and game-changing blockchain tech and turned the financial world on its head.

Trusted Third Parties

Satoshi Nakamoto explains that the web relies on trusted third parties (such as banks) to process electronic payments. But this approach leads to problems such as reversibility of transactions and high transaction fees. Moreover, the system accepts fraud as inevitable and this imposes costs on everyone.

He argues that there's a better approach that lets parties transact directly with each other. This can be accomplished by creating a peer-to-peer network where trust is replaced by verification. Transactions would also be irreversible. To secure the network, decentralized computers (i.e., nodes or miners) would provide computational proof of the chronological order of the transactions.

All transactions would be broadcast to the entire network, and everyone would adhere to the same timeline of transactions. This single version of reality (or database) would give users confidence that the electronic records, namely the blockchain, are accurate and valid.

It's crucial that everyone agrees to the same timeline of events. Thus, a timestamp server would chronologically order the transactions.

A proof-of-work system would require computing nodes to solve math puzzles, preventing any one party from flooding the system. Nakamoto says it'd be difficult for a hacker to succeed because computers will always look for longer chains (that have already completed proof-of-work) as the valid record. This sequence of block chains makes Bitcoin transactions irreversible.

Double-Spend Problem

Prior to Bitcoin, the double-spend problem prevented organizations from creating electronic currency or e-cash. The problem refers to the possibility of a user spending the same digital token more than once. It would harm a virtual economy if one token can be spent several times because the coin wouldn't be reliable.

Satoshi Nakamoto proposed ground-breaking solutions that have since revolutionized the digital economy.

First, all transactions must be made public.

Second, everyone in the network must agree to the same timeline — that there be a single version of the order in which transactions are received. For example, sending the same coin to two different merchants wouldn't work because different timestamps would invalidate the second (double-spend) payment.

In other words, get everyone on the same page whereby each node (miner) can assess that transactions are valid (or not). Everyone should also be on the same timeline so that invalid payments can be prevented and/or discovered by way of unique timestamps.

Nakamoto lists the steps for running the peer-to-peer network: New transactions are broadcast to all computers in the network. Additionally, each computing node processes transactions into a block, forming a blockchain. A block is legitimate only if all transactions in it are valid and not already spent.

Incentives For Miners

Since there is no central authority that distributes bitcoins, incentives for nodes (miners) include rewarding them with bitcoins for maintaining and securing the network. Incentives (new coins) is the mechanism by which bitcoins are brought into circulation.

Satoshi Nakamoto says the above processes add value because of the time and resources expended to make bitcoins possible, similar to gold mining:

The steady addition of a constant of amount of new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is CPU time and electricity that is expended ….

"Once a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees and be completely inflation free.

Bitcoin isn't free, and it's also expensive to create. That makes it a usable store of value and medium of exchange over a trustless, peer-to-peer network. Unlike sovereign fiats that are issued by governments and central banks, Bitcoin is inflation-free.

Nakamoto says the network's reward system encourages nodes to stay honest, and that attackers would have a difficult time tampering with Bitcoin.

[A potential hacker] ought to find it more profitable to play by the rules, such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth.

Privacy

On privacy, the author says that traditional banks achieve privacy by limiting access to information. With Bitcoin, privacy is achieved by keeping public keys anonymous. Outsiders can see sending and receiving amounts between addresses, but transactions are not linked to any identity.

Satoshi Nakamoto ends the whitepaper with a concluding statement.

We have proposed a system for electronic transactions without relying on trust ….

"The network is robust in its unstructured simplicity. Nodes work all at once with little coordination. They do not need to be identified, since messages are not routed to any particular place and only need to be delivered on a best effort basis.

It's worth repeating this statement because it may reverberate throughout the ages: *"The (Bitcoin) network is robust in its unstructured simplicity."*

Summary of 2007-08 Financial Crisis

By the summer of 2007, global financial markets had begun to show signs that the bill for a years-long binge on cheap credit was coming due. Two Bear Stearns hedge funds had collapsed, BNP Paribas was warning investors that they might not be able to withdraw money from two of its funds, and the British bank Northern Rock would soon seek emergency funding from the Bank of England.

Yet despite the warning signs, few investors suspected that the worst crisis in nearly eight decades was about to engulf the global financial system, bringing Wall Street's giants to their knees and triggering the Great Recession. It was an epic financial and economic collapse which cost many ordinary people their jobs and retirement accounts.

Sowing the Seeds

The seeds of the financial crisis were planted during years of rock-bottom interest rates that fueled a housing bubble in the U.S. and elsewhere. Faced with the bursting of the dot-com bubble, a series of corporate accounting scandals and the Sept. 11 terrorist attacks, the Federal Reserve lowered the Federal funds rate from 6.5% in May 2000 to 1% in June 2003 —flooding the economy with cheap money.

The result was an upward spiral in home prices as borrowers took advantage of the low mortgage rates, and even subprime borrowers were able to realize the dream of buying a home. Lenders then sold those loans on to Wall Street banks, which packaged them into what were billed as low-risk financial instruments such as mortgage-backed securities and collateralized debt obligations (CDOs). Soon a big secondary market for originating and distributing subprime loans developed.

Fuelling greater risk-taking among banks, the Securities Exchange Commission (SEC) in October 2004 relaxed the net capital requirement for five investment banks—Goldman Sachs (NYSE:GS), Merrill Lynch (NYSE:MER), Lehman Brothers, Bear Stearns and Morgan Stanley (NYSE:MS)—which freed them to leverage up to 30 times or even 40 times their initial investment.

Signs of Trouble

Eventually interest rates started rising and home ownership reached a saturation point. The Fed started raising rates in June 2004, and two years later the Federal funds rate had reached 5.25%, where it remained until August 2007.

There were early signs of distress. By 2004, U.S. homeownership had peaked at 69.2%. Then, during early 2006, home prices started to fall, which led to a 40% decline in the U.S. Home Construction Index during 2006. Not only were new homes being affected, but many subprime borrowers with adjustable interest rates couldn't handle the higher rates and started defaulting on their loans.

As 2007 got under way, one subprime lender or another was filing for bankruptcy. During February and March, more than 25 subprime lenders did so. In April, well-known New Century Financial, which specialized in sub-prime lending, filed for bankruptcy and laid off half of its workforce.

By June, Bear Stearns stopped redemptions in two of its hedge funds, prompting Merrill Lynch to seize $800 million in assets from the funds.

But even this was a small matter compared to what was to happen in the months ahead.

August 2007: The Dominoes Start to Fall

It became apparent by August 2007 that the financial market could not solve the subprime crisis and the problems spread beyond the U.S.'s borders. The interbank market froze completely, largely due to prevailing fear of the unknown amidst banks. Northern Rock had to approach the Bank of England for emergency funding due to a liquidity problem. In October 2007, Swiss bank UBS became the first major bank to announce losses—$3.4 billion—from sub-prime related investments.

In the coming months, the Federal Reserve and other major central banks would take coordinated action to provide billions of dollars in loans to global credit markets, which were seizing up dramatically as asset prices fell and financial institutions struggled to assess the value of the trillions of dollars worth of now-toxic mortgage-backed securities.

March 2008: The Demise of Bear Stearns

By the winter of 2008, the U.S. economy was in a full-blown recession and, as financial institutions' liquidity struggles continued, global stock markets were tumbling the most since the Sept. 11 terrorist attacks. In January 2008, the Fed cut its benchmark rate by three quarters of a percentage point — its biggest cut in a quarter century, as it sought to slow the economic slide.

The Fed started slashing the discount rate as well as the funds rate, but bad news continued to pour in from all sides. In February, the British government was forced to nationalize Northern Rock. In March, global investment bank Bear Stearns, a pillar of Wall Street that dated to 1923, essentially collapsed and was acquired by JP Morgan Chase for pennies on the dollar.

September 2008: The Fall of Lehman Brothers

By the summer of 2008, carnage was widespread across the financial sector. IndyMac Bank became one of the largest banks ever to fail in the U.S., and the country's two biggest home lenders—Fannie Mae and Freddie Mac—had been seized by the U.S. government.

Yet the collapse of the venerable Wall Street bank Lehman Brothers in September marked the largest bankruptcy in U.S. history, and for many was a symbol of the devastation caused by the global financial crisis. That same month, financial markets were in free fall, with the major U.S. indexes suffering some of

their worst losses on record as the Fed, Treasury Department, White House and Congress struggled to put forward a comprehensive plan to stop the bleeding and restore confidence in the economy.

The Aftermath

The Wall Street bailout package was approved in the first week of October 2008. Its passage stabilized stock markets, which would hit bottom in March 2009 and begin the longest bull market on record. Still, the economic damage was immense. Though the Great Recession officially ended in 2009, many ordinary people suffered from its effects for years after as the job market was slow to recover and housing prices remained suppressed.