Re: Bitcoin P2P e-cash paper

Satoshi Nakamoto | Thu, 13 Nov 2008 19:34:25 -0800

James A. Donald wrote:

> It is not sufficient that everyone knows X. We also
> need everyone to know that everyone knows X, and that
> everyone knows that everyone knows that everyone knows X
> - which, as in the Byzantine Generals problem, is the
> classic hard problem of distributed data processing.

The proof-of-work chain is a solution to the Byzantine Generals' Problem. I'll try to rephrase it in that context.

A number of Byzantine Generals each have a computer and want to attack the King's wi-fi by brute forcing the password, which they've learned is a certain number of characters in length. Once they stimulate the network to generate a packet, they must crack the password within a limited time to break in and erase the logs, otherwise they will be discovered and get in trouble. They only have enough CPU power to crack it fast enough if a majority of them attack at the same time.

They don't particularly care when the attack will be, just that they all agree. It has been decided that anyone who feels like it will announce a time, and whatever time is heard first will be the official attack time. The problem is that the network is not instantaneous, and if two generals announce different attack times at close to the same time, some may hear one first and others hear the other first.

They use a proof-of-work chain to solve the problem. Once each general receives whatever attack time he hears first, he sets his computer to solve an extremely difficult proof-of-work problem that includes the attack time in its hash. The proof-of-work is so difficult, it's expected to take 10 minutes of them all working at once before one of them finds a solution. Once one of the generals finds a proof-of-work, he broadcasts it to the network, and everyone changes their current proof-of-work computation to include that proof-of-work in the hash they're working on. If anyone was working on a different attack time, they switch to this one, because its proof-of-work chain is now longer.

After two hours, one attack time should be hashed by a chain of 12 proofs-of-work. Every general, just by verifying the difficulty of the proof-of-work chain, can estimate how much parallel CPU power per hour was expended on it and see that it must have required the majority of the computers to produce that much proof-of-work in the allotted time. They had to all have seen it because the proof-of-work is proof that they worked on it. If the CPU power exhibited by the proof-of-work chain is sufficient to crack the password, they can safely attack at the agreed time.

The proof-of-work chain is how all the synchronisation, distributed database and global view problems you've asked about are solved.

Previous message | View by thread | View by date | Next message

- Re: Bitcoin P2P e-cash paper *James A. Donald*
- Re: Bitcoin P2P e-cash paper *Satoshi Nakamoto*
- Re: Bitcoin P2P e-cash paper *Satoshi Nakamoto*
- Re: Bitcoin P2P e-cash paper *James A. Donald*
- Re: Bitcoin P2P e-cash paper *Satoshi Nakamoto*
- Re: Bitcoin P2P e-cash paper *James A. Donald*
- Re: Bitcoin P2P e-cash paper *Satoshi Nakamoto*
- Re: Bitcoin P2P e-cash paper *Satoshi Nakamoto*
- Re: Bitcoin P2P e-cash paper *James A. Donald*
- Re: Bitcoin P2P e-cash paper *"Hal Finney"*
- Re: Bitcoin P2P e-cash paper *Satoshi Nakamoto*
- NSA history *Charles Jackson*
- WSJ Story on NSA history *Charles Jackson*
- Re: Bitcoin P2P e-cash paper *Ray Dillinger*
- Re: Bitcoin P2P e-cash paper *James A. Donald*
- Re: Bitcoin P2P e-cash paper *Satoshi Nakamoto*
- Re: Bitcoin P2P e-cash paper *James A. Donald*
- Re: Bitcoin P2P e-cash paper *Satoshi Nakamoto*
- Re: Bitcoin P2P e-cash paper *Ray Dillinger*
- Re: Bitcoin P2P e-cash paper *Nicolas Williams*
- Re: Bitcoin P2P e-cash paper *Satoshi Nakamoto*

Reply via email to

Satoshi Nakamoto