Bitcoin Explained

by Andy Greenberg via bill - Forbes *Monday, Jun 20 2011, 10:18am*
international / miscellaneous / other press

Digital cryto-currency may replace valueless fiat currency

> Bitcoin is a grassroots nonprofit project that seeks to fashion a new currency out of little more than cryptography, networking and open-source software, and Gavin Andresen is the closest thing the project has to a director. Bitcoin is not, he explains, just a new way to digitally spend dollars, pounds or yen. That's been tried before.

Bitcoin is different: It wholly replaces state-backed currencies with a digital version that's tougher to forge, cuts across international boundaries, can be stored on your hard drive instead of in a bank, and--perhaps most importantly to many of Bitcoin's users--isn't subject to the inflationary whim of whatever Federal Reserve chief decides to print more money.

"Bitcoin is designed to bring us back to a decentralized currency of the people," says Andresen, a 44-year-old software developer and entrepreneur based in Amherst, Mass. "This is like better gold than gold."

As with shiny-metal-backed currencies, Bitcoins derive their value partly through their scarcity, which is defined not by how much can be dug up with shovels but by a cryptographic lottery. Anyone can get Bitcoins without paying cash for them by downloading and running Bitcoin's "mining" program. The machines in Bitcoin's mining network, now in the thousands, compute an encryption function called a "hash" on a set of random numbers, and coins are awarded every ten minutes to whichever miner happens to compute a number below a certain threshold.

That lottery tightly controls how many Bitcoins are created. There are currently close to 6 million in existence. By 2014 there will be about twice that number. Bitcoin's distributed software is set to slow production over time so that there will never be more than 21 million in circulation. "No banker can control it. No evil dictator tyrant can print zillions and destroy the value," says Bruce Wagner, organizer of New York's Bitcoin developer's meet-up.

Of course, the other factor that determines the worth of a currency is whether anyone will accept it in exchange for goods and services. And for Bitcoin, a subculture of geek-friendly merchants is catching on. About $30,000 worth of Bitcoins change hands every day in electronic transactions, spent on Web-hosting, electronics, dog sweaters and alpaca socks.

Also drugs. Particularly illegal ones. Since Bitcoins can be spent on the Internet without the use of a

bank account, they offer a convenient system for anonymous purchases. There's no centralized storage of funds, so accounts can't be frozen by law enforcement or PayPal administrators. "Illegal stuff will be a niche for Bitcoin," admits Andresen. "That bothers me, but it's just like any currency. You can't stop dollar bills from being used for the drug trade either. That's an unfortunate feature of any cashlike system."

Bitcoins' anonymity was no accident. The system was originally designed by Satoshi Nakamoto, a mysterious, privacy-obsessed figure who first described the currency's specs in a series of posts on a cryptography e-mail list in late 2008. Nakamoto declined to be interviewed for this story, and not even Andresen, who took over the project as technical lead in May 2010, has communicated with Bitcoin's founder except through e-mail and posts on Web forums. Nakamoto has compared Bitcoin to the systems of anonymous financial transactions sought by the anarchist cypherpunk movement in the 1990s, whose adherents saw cryptography as a way to shift power from institutions to individuals.

Thanks in part to its growing uses, both black- and white-market, the newborn currency is appreciating at a wild clip. In just the year since Andresen joined the project, it's jumped from half a penny in value to about a dollar.

That possibly irrational exuberance may be a sign that Bitcoin is headed for a speculative bubble. The currency already swings as much as 50% in value over some single days. But Bitcoin's supporters are confident the free market can solve that problem as Bitcoin's advantages attract more nonspeculative buying and selling.

One way they hope to bring more normals into the fold: by expanding Bitcoin's applications to the real world. Bitcoin devotees in New York's informal developer group are rolling out an Android app for mobile Bitcoin buying. They're also building open-source software that can be integrated into point-of-sale terminals.

"Someday this will probably have the Fed scrambling," says the New York meet-up's Bruce Wagner. "They still don't know what Twitter is. By the time they figure this out, it will have already taken hold."

http://tinyurl.com/3c9c7q5
