15 APRIL 2018|ARTICLES

Who is Nick Szabo?

By PAUL ANDREW published on: coincentral.com

https://coincentral.com/who-is-nick-szabo/

Nick Szabo

Nick Szabo, the inventor of smart contracts and Bit Gold, laid the foundation for the creation of Bitcoin. He defined smart contracts 14 years before Bitcoin. Then he theorized bits having value based on proof of work 5 years before Bitcoin.

With degrees in both computer science and law, and an intense fascination in the history of money, it is no surprise Nick Szabo was ahead of his block time. His ideas on the history and future of money, including the role of cryptocurrency, are well documented on his blog. Satoshi acknowledged that Bitcoin was based on Nick's work, but many believe that Satoshi is, in fact, Nick Szabo.

History of Money

Nick's analysis of the origins of money provides insight into the future of cryptocurrency. He explains the logical emergence of currency and the inevitable equilibrium of multiple currencies. Szabo argues that every transaction contains a "mental cost." In a world of "pure barter," you would need to memorize roughly N squared prices for N different commodities. For example, imagine a world with only brick, wheat, sheep, and gold. You would need to know the price of each item in terms of each other item. To reduce the mental cost, humans would eventually "converge on a single currency" within that society. Mental costs would dramatically decrease. Now you would only need to know the price of each item in terms of the single currency.

Multiple Currency Equilibrium

As each society converges to their own currency, we end up in a world with multiple currencies. We've seen this play out in cryptocurrencies. Historically doing "business in a world of multiple currencies, much less of pure barter, has always led to confusion, error, and overly complex accounting... But with sufficiently low mental transaction costs and sufficiently unpredictable exchange rates, it pays to hang on to multiple currencies, and a world of multiple currencies is the equilibrium."

Nick argues the exchange rates of different currencies fluctuate and are unpredictable. Therefore, it behooves you to hold multiple currencies. Many want Bitcoin to win out as the one world currency. However, Nick argues technology would further cement the existence of multiple currencies. "Now for a more radical claim: in some cases, computers can drastically reduce the mental transaction costs of comparing prices in multiple currencies, which along with the 'costless teleportation' of online markets allows multiple currencies or in some cases even barter to become the equilibrium."

Nick writes about an unending variety of topics. He explored the different physical objects used to represent money throughout history. He also writes about the "traditions of non-governmental money."His interests do not revolve entirely around money though. Nick is still a fun guy, publishing a book on the fungus of East Bay California.

Smart Contracts

In 1995, Nick coined the term "smart contract" as "a set of promises, including protocols within which the parties perform on the other promises. The protocols are usually implemented with programs on a computer network, or in other forms of digital electronics. Thus these contracts are "smarter" than their paper-based ancestors. No use of artificial intelligence is implied."

He refers to contracts in the traditional sense as wet code. They can be interpreted differently and laws are different based on the jurisdiction. In addition, a traditional contract can be difficult to enforce. **Smart contracts would be the "dry code," precise and securely stored on a blockchain.** In 1996 he went into further detail analyzing the advantages and disadvantages of smart contracts as "building blocks for digital markets." Given the popularity of Ethereum today, it's clear there is a high demand for the actual implementation of these smart contracts. An Ethereum unit is named after Szabo to recognize this contribution.

Unit	Wei Value	Wei
wei	1 wei	1
Kwei (babbage)	1e3 wei	1,000
Mwei (lovelace)	1e6 wei	1,000,000
Gwei (shannon)	1e9 wei	1,000,000,000
microether (szabo)	1e12 wei	1,000,000,000,000
milliether (finney)	1e15 wei	1,000,000,000,000,000
ether	1e18 wei	1,000,000,000,000,000,000

Bit Gold

In 1998, Szabo theorized Bit Gold, a way to convert bits and computing power into something of storable value. “I started thinking about the analogy between difficult-to-solve problems and the difficulty of mining gold. If a puzzle took time and energy to solve, then it could be considered to have value. The solution could then be given to someone as a digital coin.”

Bit gold used devoted computing power to solve cryptographic problems with the solution becoming part of the next problem. Here are the main steps that Szabo outlined:

(1) Create a public string of bits known as the “challenge string” (see step 5).

(2) Alice on her computer generates the proof of work string from the challenge bits using a benchmark function.

(3) The proof of work is securely timestamped. This should work in a distributed fashion, with several different timestamp services so that no particular timestamp service need be substantially relied on.

(4) Alice adds the challenge string and the timestamped proof of work string to a distributed property title registry for bit gold. Here, too, no single server is substantially relied on to properly operate the registry.

(5) The last-created string of bit gold provides the challenge bits for the next-created string.

(6) To verify that Alice is the owner of a particular string of bit gold, Bob checks the unforgeable chain of title in the bit gold title registry.

(7) To assay the value of a string of bit gold, Bob checks and verifies the challenge bits, the proof of work string, and the timestamp.

Bit Gold to Bitcoin

The parallels to Bitcoin are astounding. You can see the use of proof of work, solutions becoming part of the next challenge and a distributed ledger of who owns each string of bits. **However, there were some key differences between Bit Gold and Bitcoin.**

With Bitcoin, a miner finding a solution to the cryptographic puzzle receives Bitcoins as a reward. With Bit Gold, the solution to the puzzle, a string of bits, is the reward. Each string would have different value depending on the length and difficulty of finding it. Thus the strings lacked fungibility, adding a mental cost to transactions. Unfortunately, the details of Bit Gold were never fully worked out. On December 27th, 2008 Szabo wrote, "Bit Gold would greatly benefit from a demonstration, an experimental market (with e.g. a trusted third party substituted for the complex security that would be needed for a real system). Anybody want to help me code one up?"

One week later on January 3rd, 2009, Satoshi released the code for Bitcoin, with Bit Gold as the inspiration.

Satoshi Rumors

Rumors often swirl that Szabo is Satoshi Nakamoto. The rumors often refer to his affinity for currency and skills in computer science. A researcher analyzed the writing style of both Nick and Satoshi and declared Szabo as the number one candidate to be Satoshi.

Countless articles accuse Nick Szabo of being Satoshi Nakamoto, accusations that of course, Szabo denies. He said in response to an article, "I'm afraid you got it wrong doxing me as Satoshi, but I'm used to it." At this point, it's quite clear Satoshi wished to remain anonymous and thus there won't be further conjecture here on the true identity.

Second Layer Solutions

With a lightning bolt in his twitter name, Szabo is a strong supporter of the lightning network and second layer solutions for scaling the Bitcoin. Slow Bitcoin transaction times and expensive fees are a result of high demand for the network and blocks becoming full. The Bitcoin Cash scaling approach is to simply increase the block size, a strategy Nick argues against.

When commenting on block sizes, Szabo said there is an "obsessive group of people who think of this as some artificial barrier to more transactions per second on bitcoin. Really it's job is it's a fence preventing people from overwhelming, flooding, the network with lots of transactions that the full nodes cant handle. That transaction history keeps building and building. As we increase the amount of people that can make transactions, we decrease the amount of computers that can handle the transactions."

With increased block sizes, the number of computers able to run a full node would decrease, increasing centralization of Bitcoin. Szabo is quite wary of the dangers associated with centralization, saying "every time a money becomes more a medium of censorship, it becomes less a medium of exchange."

Szabo commented further on scaling, saying "at scale, you can't pay for coffee on a premium global blockchain. You'll need a peripheral financial network that settles on that blockchain. Can be confident that if one secure blockchain was used for all world's high-value transactions, fees would be too high." Fortunately, with new investment and continued work, the lightning network continues to make progress.

Finally, Szabo said the block size "shouldn't even be a public debate."

Final Thoughts

Szabo's understanding of money, history, and cryptocurrency makes his writings an invaluable resource for those interested in blockchain technology. One of his most powerful quotes helps us understand the importance of Bitcoin's fixed supply of 21 million coins. "**In summary, all money mankind has ever used has been insecure in one way or another. This insecurity has been manifested in a wide variety of ways, from counterfeiting to theft, but the most pernicious of which has probably been inflation**." As someone who has made their mark on cryptocurrency for over 20 years now, it's certainly worth paying attention to Nick Szabo's insight moving forward.