Bitcoin: A Green Paper for Core Services

By Gregg Zigler

[*Note: proprietary information has been redacted*]

In Q2 of 2013, PayPal executives started talking about Bitcoin in the press. David Marcus ("we're kinda thinking about it"), John Donahoe ("we're looking at Bitcoin closely"), and James Barrese ("if Bitcoin comes to a critical mass, we would look at how we would enable it") all gave us a warning that we should be prepared to support crypto-currencies in Core Services.

Overview and business risks

In a 2008 paper, the pseudonymous Satoshi Nakamoto published the principles and source code of Bitcoin. With Bitcoin, an algorithm determines the rate at which some of the 21 million possible bitcoins will be generated ("mined"). Wallet clients publish transactions on a decentralized peer-to-peer network, and miners publish confirmations of those transactions on the same network in a ledger ("block chain"). No single node on the network is trusted, but 51% of active nodes at any instant are trusted to prevent counterfeiting and "double spending". Clients use public key cryptography to sign transactions sent from one public key ("bitcoin address") to another.

Outside of Satoshi's core protocol, various services link Bitcoin to other financial networks. **Payment processors** like BitPay and Coinbase connect buyers and merchants to the network where, for a fee, miners compete to confirm transactions in the next block in the block chain. **Exchanges** like Mt.Gox exchange BTC for traditional fiat currency such as USD and JPY. **Wallets** like Bitcoin-Qt and Blockchain.info provide mobile and desktop applications that manage private crypto-keys and connections to the network.

Mixing services like BitLaundry and LocalBitcoins "enhance anonymity" by routing transactions through additional layers of wallets or by connecting users for face-to-face exchange of bitcoins and dollars. **Competitors** like Litecoin and PPCoin address critiques of the Bitcoin protocol such as high-energy consumption and trends toward expensive mining hardware.

Bitcoin's increasing visibility continues to attract the attention of regulators. For example, FinCEN recently seized Wells Fargo and Dwolla accounts of Japan-based Mt.Gox for failure to register as a money transmitter in the US. And the State of California sent a cease and desist letter to the Bitcoin Foundation for the same reason.

At the same time, the exchange rate of BTC has been very volatile. Since the beginning of 2013, rates have gone from $20 USD to as high as $230 USD to a current $100 USD, with a few huge intra-day price swings.

Protocol and technical risks

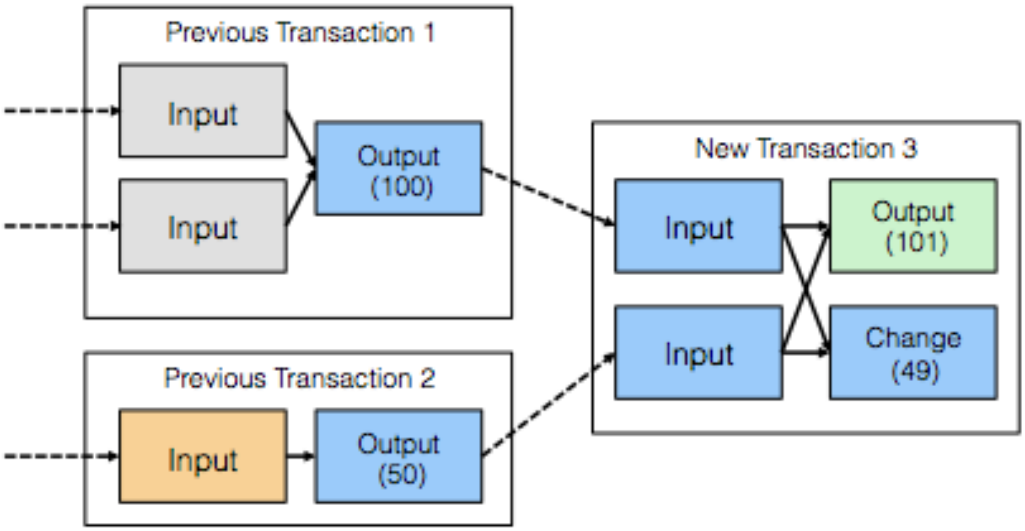
The peer-to-peer network has no central authority. All transactions are published to and persisted in the block chain, so

anyone connected to the network can easily calculate how much money any given bitcoin address owns.

PAYMENT CARD	SIMILAR BITCOIN CONCEPT
Pull funds model	Push funds model, like unilateral Send Money
Authorization	Sender signs and broadcasts transaction.
Capture	None. Sender publishes a single message, like pinless debit.
Settlement	Miner confirms transaction. No single confirmation is authoritative. A new block of confirmations occurs once every 10 minutes, and many clients wait one hour before treating a payment as complete.

The protocol differs in other ways from a typical payment card network. Most notable is the absence of chargeback or any mechanism to reverse a payment. Another difference is that statistics and risk tolerance determine how soon most clients consider a payment to be complete. One rogue miner may fake the confirmation of an invalid payment. But within an hour, 51% of the miners will confirm a longer, alternate block chain, and the rogue confirmation will be ignored.

Each bitcoin can be subdivided into 100 million units ("satoshi"), and a payment may combine funds from multiple bitcoins and multiple bitcoin addresses. When a payment does not consume all bitcoins previously received in the source transaction(s), then the sender must explicitly give himself "change" in the transaction. For example, when combining funds from two previous transactions totaling 150 BTC in order to send 101 BTC to a friend, I must also send myself 49 BTC in change.



Consumers face a risk related to public key cryptography, when the private keys are stored in a file on their desktop or mobile device. Any malware that can read that file can also spend that money. No chargeback, no reversal, no central authority can help recover the money.

Satoshi envisioned that so many worldwide commodity servers would run the protocol, that no regulator or miner could possibly control it. But because miners now use high-end GPU hardware, and soon custom ASIC chips, the power of the network may become concentrated into a few hands, hence attracting regulators. Similarly, a few dishonest miners could conspire, launch a DDOS attack against the rest, achieve 51% of active mining nodes, and insert bad blocks into the block chain.

Similarities with PayPal

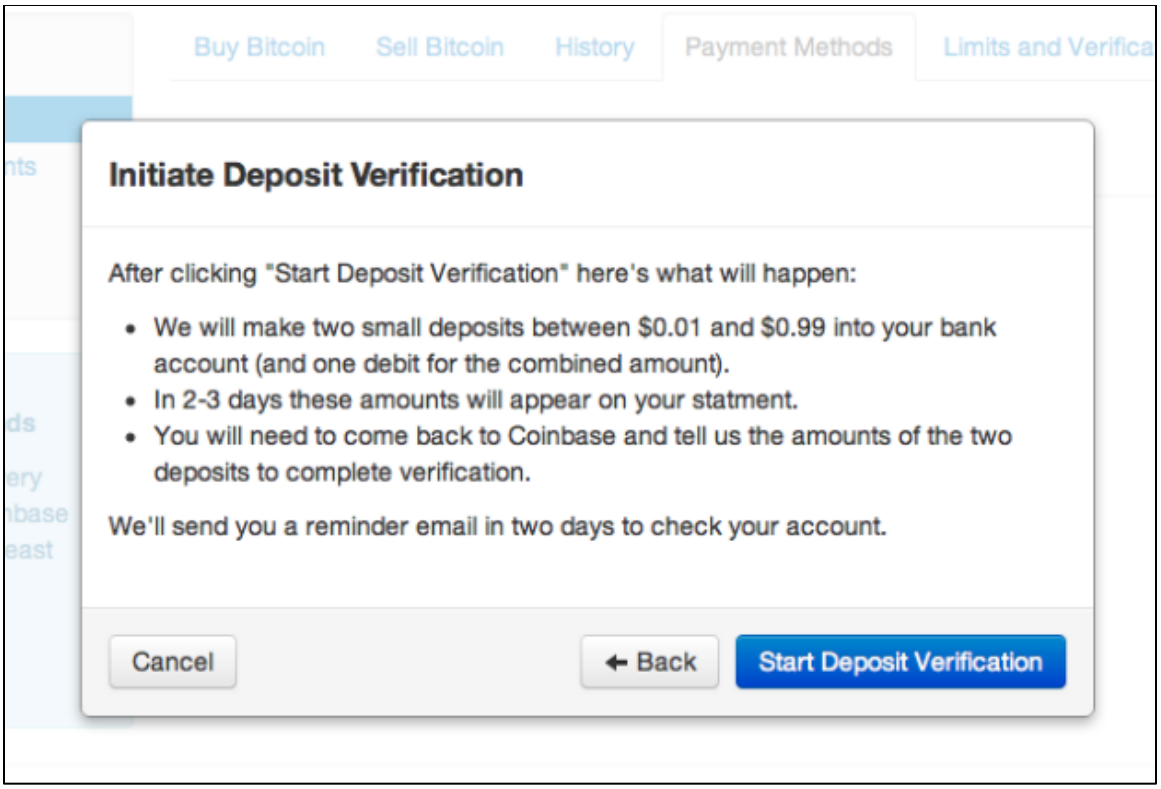
Eric Jackson's book "The PayPal Wars" paints a picture of PayPal in 1999 that looks very similar to Bitcoin today.

	BITCOIN 2013	PAYPAL 1999-2002

Philosophical Basis	Cypherpunk: strong cryptography for political change.	Libertarian: wary of concentrated government
Technological Basis	Public key cryptography	Public key cryptography
Business Markets	Popular in underground economy	Popular in gaming and adult industries
Developers	Many value privacy and anonymity	Many had copy of *Cryptonomicon*, a sci-fi novel about electronic money
Shutdown Due to Licensing Issues	California	Louisiana, New York

In 1999, PayPal co-founder Peter Thiel dreamed that "*… PayPal will give citizens worldwide more direct control over their currencies than they ever had before. It will be nearly impossible for corrupt governments to steal wealth from their people through their old means …*". But starting in 2005, PayPal instead spent [*redacted*] to implement the restrictions required by the governments of Brazil, Russia, India, China, and other countries wherever we expanded. In May of this year, Peter Thiel invested $2 million in BitPay, a Bitcoin payment processor.

The bitcoin.it wiki writes that wallet service Coinbase is modeled to provide an experience familiar to those who are comfortable using PayPal. Indeed, Coinbase supports send money, request money, add funds, and even bank confirmation using two small random deposits, just like PayPal.



Possible business capabilities

[*redacted*]

Call to action

As payment professionals, each of us should experiment with crypto-currencies, even if we spend only a few dollars. For example:

- Sign up for a Bitcoin or Litecoin account
- Pay for something at a POS using BTC
- Join a mining pool

The more Core Services understands crypto-currencies, the more quickly we can respond to the BU when they ask for support.