Pipeline
Technology for Service Providers.
www.pipelinepub.com Volume 14, Issue 2

Patent Pipeline: Bitcoin Has Spurred Digital Currency Technologies

By: Alec Schibanoff

You cannot avoid Bitcoin. It is in the news every day, and the more volatile the pricing of this leading digital currency or cryptocurrency (the terms are interchangeable), the more news it generates. While Bitcoin is just one of the emerging digital currencies – there is also Ethereum, Litecoin, Zcash, Dash, Ripple and Monero – Bitcoin has zoomed to the top to be the leading cryptocurrency.

Bitcoin has a mind-blowing Market Cap of $144 billion. Yes, billion with a "B." All of the issued Bitcoins in circulation (16,861) times the average value of one Bitcoin ($8,595 as of the writing of this article) is how one gets to a market capitalization of $114 billion! Bitcoins cannot be ignored, and the Innovation Community has not ignored them.

In this edition of Patent Pipeline, we look into the future of the Bitcoin by looking at four U.S. Patents that cover Bitcoin-related technologies.

Bitcoin-accepting gaming machines

U.S. Patent No. 8,449,378 for a "Gaming system, gaming device and method for utilizing bitcoins" is one of two Bitcoin gaming patents from IGT (International Gaming Technology), the leading manufacturer of gaming equipment such as slot machines and computerized Poker and Blackjack machines. This patent was published in 2013 and has 20 Claims. While the title of the patent references "Bitcoins," the claims in the patent are much broader.

This patent is cleverly written to include not just Bitcoins, but any digital currency, as well as any "wagering game" that can be played on a display device. So, that covers everything from slot machines to computer Poker. The patent permits the user to play with Bitcoins or other digital currencies, and be paid his or her winnings in Bitcoins or other cryptocurrency. The gaming device described in the patent includes a video console, an input device, and a processor. The process covered by the patent is to (a) receive a wager of an amount in a specific currency on a play of a wagering game, (b) have the processor execute a plurality of instructions to generate an outcome for the play of the wagering game, (c) have the console display the generated outcome of the play of the wagering game, and (d) provide an award – if the player wins – to be paid out in the specific currency the game user started with.

It will be just a matter of time before casinos – both physical and online – will be accepting digital currency, most likely starting with Bitcoin.

Bitcoin ATM

U.S. Patent No. 9,135,787 for a "Bitcoin kiosk/ATM device and system integrating enrollment protocol and method of using the same" creates the first ATM specifically for buying and selling Bitcoins. The patent is from two independent inventors, John and Mark Russell, it was published in 2013, and it has 12 Claims.

The invention is most comprehensive. It includes a bill validator, a bill dispenser, a user interface, a biometric interface, an ID scanner/reader, a camera, and a processor programmed to run executable instructions – many of the same elements that make up a conventional ATM, except for

its ability to accept and dispense Bitcoins. The patent also includes a carefully defined security methodology for insuring the identity of each user. It starts with the input of the customer's mobile phone number via the user interface, followed by the transmission of a text message that includes a random code to the mobile phone of the customer. Next steps include verification of the random code that was sent to the customer via the user interface to confirm that customer's mobile phone number; input of a PIN from the customer via the user interface; input of biometric data such as a palm print from the customer; an image of the customer (captured via the Bitcoin ATM's camera); and verification of the identity of the user from a driver's license or other form of photo ID using the machine's ID scanner/reader.

Shortly after the publication of this patent, Bitcoin ATMs started showing up – the latest estimate is that there are about 1,500 of them in use today – that use many of the elements in the patent. Those manufacturers and owner/operators will clearly have to take a license for this Patent!

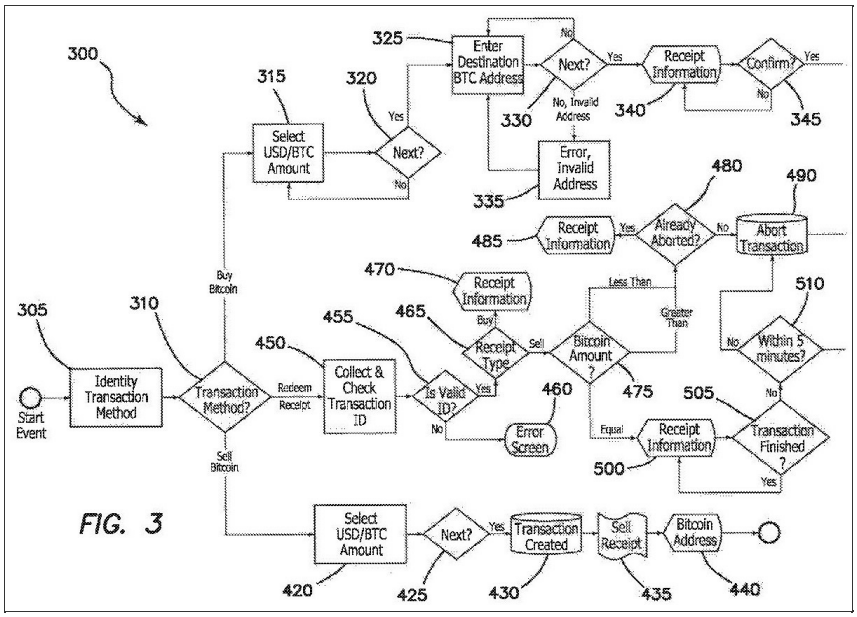

Figure 3A from U.S. Patent No. 9,135,787 is a flow chart that illustrates the identify verification routine covered by the patent. Click image to expand.

Accessing Bitcoins from the blockchain

U.S. Patent No. 9,569,771 for a "Method and system for storage and retrieval of blockchain blocks using galois fields" addresses the storage and issuance of Bitcoins or other digital currency from a peer-to-peer communications network. This patent was published just last year, includes 20 claims, and comes from independent inventors Stephen and Zachary Lesavich.

To understand this patent, however, you need to first understand "blockchain" and "Galois fields." In the world of digital currency, there are NO banks, no Federal Reserve System and no mint to print the actual money. For digital currencies, the blockchain is the closest thing to a bank, but it is nothing like a bank. For starters, it does not have a physical location and it is not static, but a continuously growing list of records called "blocks" that are linked together (that's the "chain") and kept secure via sophisticated cryptography. Each block contains a cryptographic hash or algorithm that links it to the previous block along with a timestamp for the transactions from that block. A proper blockchain is inherently resistant to any modification of the data in the blocks. A blockchain is an open, distributed ledger that records transactions between two parties very efficiently and in a verifiable and permanent way. To access the distributed ledger, a blockchain must be managed by a peer-to-peer network that adheres to a pre-defined protocol for the validation of new blocks in the blockchain. Once it is recorded, the data in a specific block cannot be altered after the fact without the altering all subsequent blocks. Since it operates in a peer-to-peer network, all blockchain transactions are fully accessible to the public. There are no private transactions in the world of digital currency, only full transparency.

A Galois field – in case you did not major in calculus – is a field (or universe) that contains a fixed number of finite numbers. Also called a "finite field," it is the basis for all basic mathematical

functions – addition, subtraction, multiplication and division. The integers in a finite field are designed as “mod p” when “p” is a prime number. Thoroughly confused? Good.

This patent provides additional security for digital currency transactions by establishing a routine under which one or more new blocks are created for a blockchain using a cloud application on a cloud server network that uses several processors. It securely stores new blocks in the blockchain in one or more cloud storage centers, and creates a modified Galois field GF(p^n) that consists of lookup table in the modified Galois field that has unique field elements, as well as a second portion of the Galois field lookup table that includes virtual network address locations, actual network address locations, virtual protocol port address designations, and actual protocol port address designations that can be used with one or more processors on the cloud communications network.

This patent covers high-end, cutting-edge technology that addresses the very real issue of hackers breaking into the blockchain and causing the digital currencies recorded there to no longer exist!

Testing transaction protocol to verify a device

Our fourth and newest property is U.S. Patent No. 9,735,958 for a “Key ceremony of a security system forming part of a host computer for cryptographic transactions.” This patent was published just last August, has just five Claims, and is assigned to Coinbase, Inc., a leading digital currency exchange. While the narrative of the Patent specifically references Bitcoins, the Claims are broadly written.

For digital currency trading firms, security is hyper-critical. This patent creates bundles for custodians of key data that are encrypted with the computer system’s custodians’ passphrases. Each bundle includes a master key share that is designed so it can also store an operational master key that is used for private key encryption during a checkout transaction and private key decryption when authorizing a payment. The bundles also include transport layer security keys for authenticating requests such as creating an application-programmable interface key for a web application so the system can be unfrozen after it has been frozen by an administrator.

If you cannot understand all of this, you definitely cannot hack into the system!

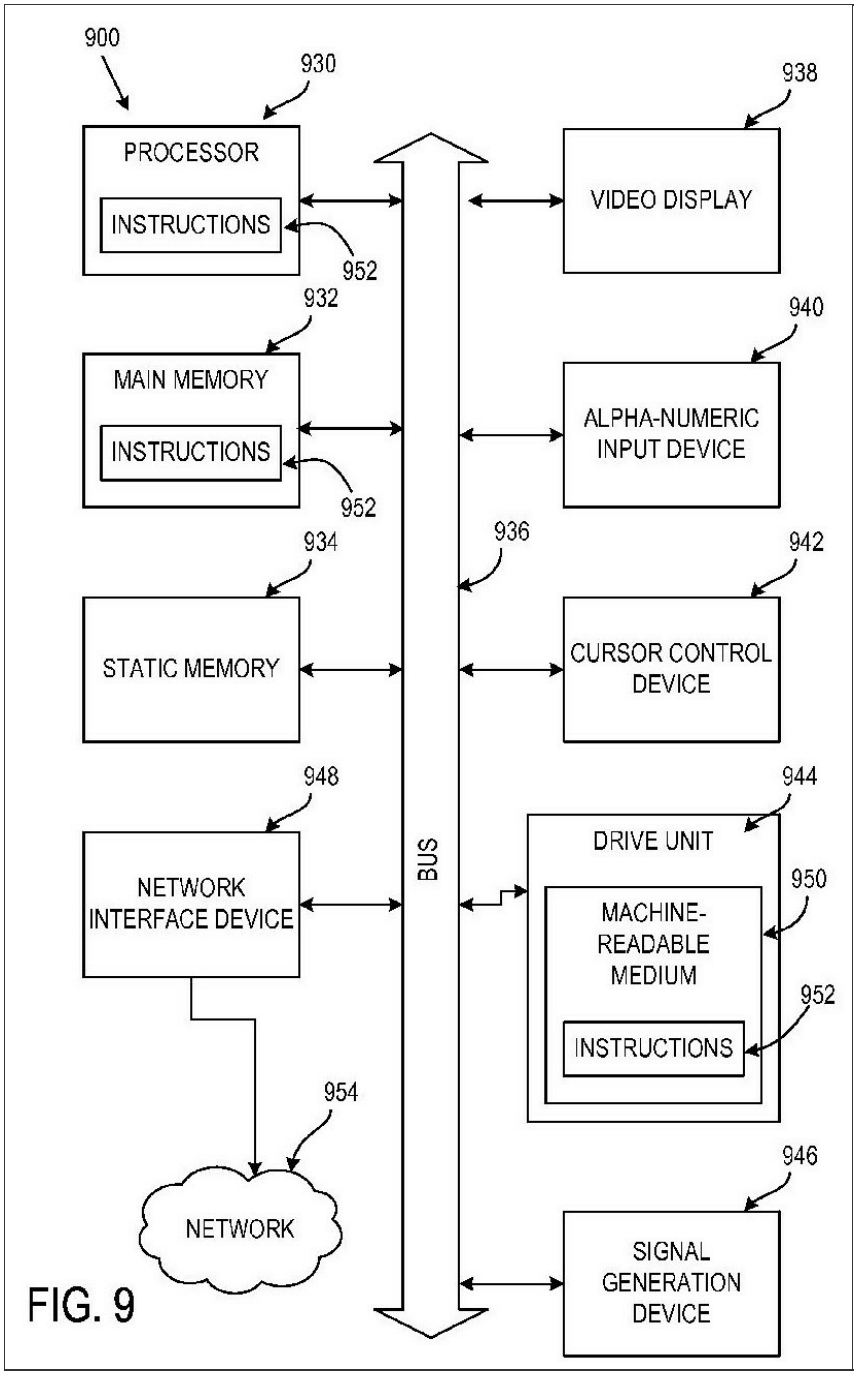

Figure 9 from U.S. Patent No. 9,735,958 is a block diagram of computer system that uses the cryptographic technology covered by this patent.

A brave new world of technology challenges

We've come a long way from cashing our pay checks and buying groceries with paper money. The Bitcoin and its sister cryptocurrencies have virtually no physical characteristics! They only exist in a cyber-virtual reality. There are no hard-copy back-up files. Processing digital currency transactions, keeping those transactions safe and secure, and maintaining the blockchain to record those transactions safely from hackers or system failures will be an ongoing challenge requiring disruptive technologies.