Bitcoin   Blockchain   FinTech   ETH   Learn

Free   PR   Widget
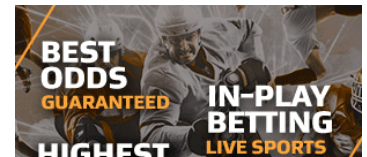
BITCOIN PRICE: 970.01 USD HIGH: 1074.69 USD LOW: 913.73 USD

Bitcoin Security   Bitcoin Technology   Blockchain News

UK Giant Seeks Patent for Invention Mitigating Blockchain Attacks

Lester Coleman on 09/02/2017

The British Telecommunications Public Limited Company (BT) has applied for a U.S. patent for a computer method for mitigating attacks against a blockchain. The method generates a notification signal to flag a malicious event and allows for remedial action, according to the filed document.

The application has been filed with the U.S. Patent and Trademark Office. Inventors are Joshua Daniel, Gery Ducatel and Theo Dimitrakos, all of London.

The application describes the invention as a computer implemented method for detecting malicious events that occur with respect to a blockchain data structure. These include defining a transaction creation profile by which transactions can be generated and submitted to the blockchain.

What Causes Attacks

The application noted malicious attacks are caused by an entity procuring sufficient computing power to control more than half of the mining resources working in the blockchain. The attacker submits a transaction that pays the merchant while mining a blockchain fork that includes a double spending transaction

Recent Posts
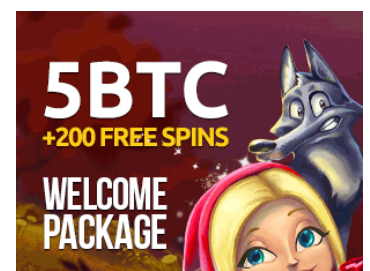
Anger Grows at PBOC's Interference with Bitcoin

FinTech Can Help Banks Tap into $500 Billion Hole

Why Bitcoin and Blockchain Are 'Relatively Safe'

Chinese Bitcoin Mining Firm Canaan to Open 10 MW Facility at Node Pole, Sweden

[Updated] Bitcoin Price Crashes as Chinese Exchanges OkCoin & Huobi Pause Withdrawals Temporarily

that includes a double spending transaction.

If the attacker controls more than half of the network hash rate, there is a 100% chance of success. Because the attacker in such a case can generate blocks faster than the rest of the network, he can persevere with his private fork until it extends past the branch built by the legitimate network.

Other attacks that can threaten the blockchain include the Sybil attack, whereby an entity fills a miner network with clients controlled centrally or by pseudonymous miners. There are also denial of service attacks that send excessive data to a miner to overwhelm him so he cannot process normal transactions.

Invention Mitigates Attacks

The invention provides a method for detecting such events.

The security component is a virtual or physical computer system or an application or service executing on a computer system communicatively connected to the blockchain. The security component generates a new data structure known as a profiler data structure for storage in the blockchain.
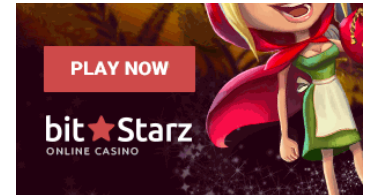
Search

Advertisement

The security component monitors the blockchain to ensure that the generation of profile transactions complies with the transaction creation profile. Such generation indicates faithful validation and execution of the profiler by miners.

Where profile transactions do not appear in the blockchain as expected, then non-compliance is detected. Such an occurrence results from miners not correctly validating and executing the profiler stored in the blockchain.

An absence of one or a few expected profile transactions warrants alarm that a malicious event has occurred. Mitigating or remedial action can then be taken. Such action can include generating an alert, communicating the non-compliance to other entities operating with the blockchain, terminating access to the blockchain, protecting assets recorded in the blockchain, and inspection of transactions.

Also read: Banks spend big to fight cybercrime, heighten efforts to supervise employee behavior

How It Deploys

The program can be implemented using a software-controlled programmable processing device, such as a

microprocessor, digital signal processor or other processing device, data processing apparatus or system.

The program can be embodied as source code or undergo compilation for implementation on a processing device, apparatus or system, or can be embodied as object code.

The program is stored on a carrier medium in device readable forms, such as solid-state memory, magnetic memory such as disk or tape, optically or magneto-optically readable memory such as compact disk, or digital versatile disk.
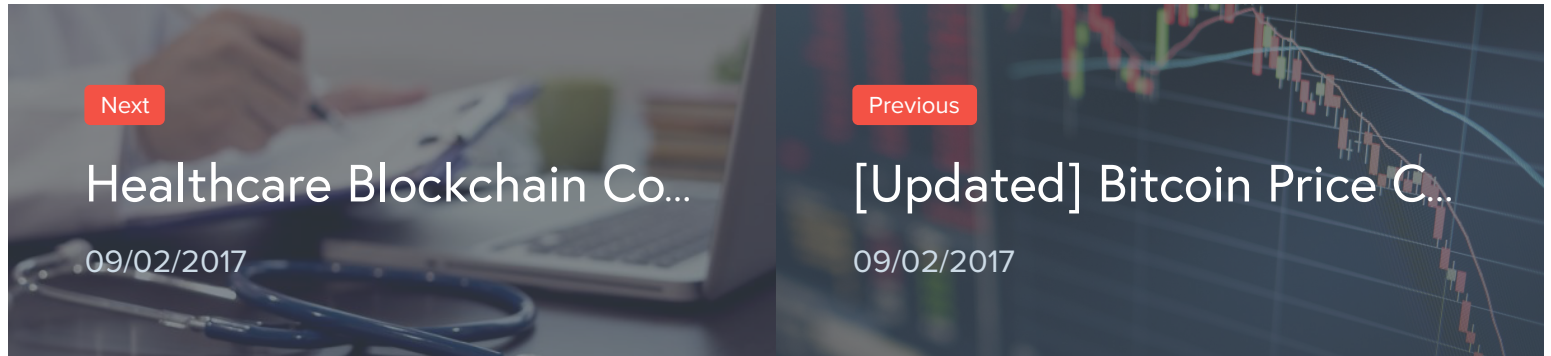
The program can be supplied from a remote source embodied in a communications medium such as an electronic signal, radio frequency carrier wave or optical carrier wave.

Image from Shutterstock.

Posted in: Bitcoin Security, Bitcoin Technology, Blockchain News, News   **Tagged in:** British Telecom, patents, Sybil, U.S. Patent & Trademark Office, uk, USPTO
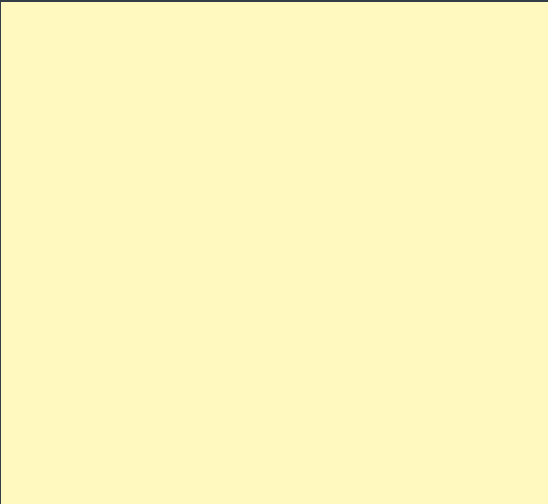
Next

Healthcare Blockchain Co...

09/02/2017

Previous

[Updated] Bitcoin Price C...

09/02/2017

Tags

apple Australia **bitcoin**
bitcoin accepted here bitcoin asic
miner **bitcoin atm** bitcoin
exchange bitcoin foundation
Bitcoin price bitcoin
regulation bitfinex bitlicense
bitpay bitstamp
blockchain block chain
Blockchain.info canada **china**
coinbase cryptocurrency
dogecoin **Ethereum**
News fintech IBM india japan
litecoin mark karpeles microsoft
mtgox **mt gox** okcoin overstock
paypal pboc R3 reddit regulation
ripple Ross Ulbricht **russia**
satoshi nakamoto security **silk
road**