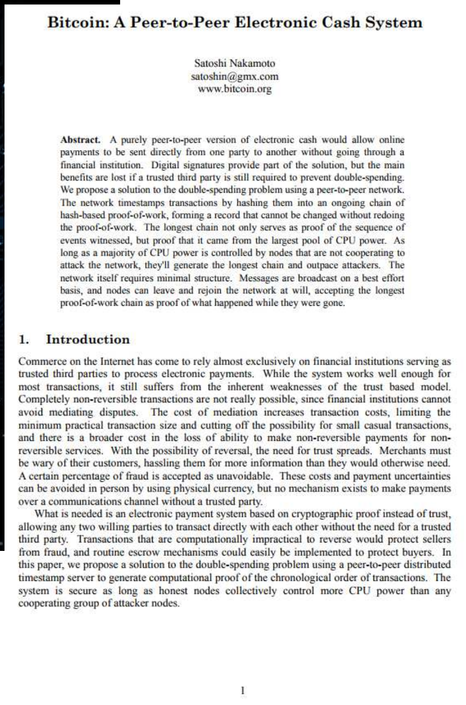
The Blockchain Revolution: Promises and Security Challenges

Bidan Zhu
Information Security Officer
Division of Nuclear Security, IAEA

Bitcoin: Satoshi Nakamoto : A Peer-to-Peer Electronic Cash System (October 31 2008)



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

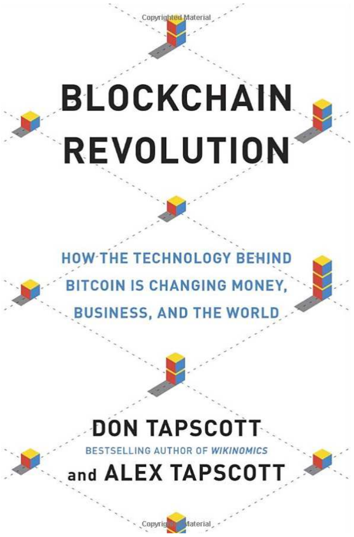
Bitcoin Pizza Day - 22 May 2010

- Bought on 22nd May 2010 by **Laszlo Hanyecz**, the Florida programmer paid a fellow Bitcoin Talk forum user **10,000 Bitcoins** for two **Papa John's pizzas**. Back then – when the technology was just over a year old – that equated to roughly $25, but is about **$75million** by today's exchange rate.
- Every Year on 22nd May, all bitcoiners in the world over celebrate the anniversary of the most expensive pizzas in history.

Laszlo Hanyecz bought these pizzas for 10,000 bitcoins on May 22, 2010. Laszlo Hanyecz

Blockchain Revolution

“The technology likely to have the greatest impact on the next few decades has arrived. And it’s not social media. It’s not big data. It’s not robotics. It’s not even AI. You’ll be surprised to learn that it’s the underlying technology of digital currencies like Bitcoin. It’s called the blockchain.” — Don Tapscott



Copyrighted Material

BLOCKCHAIN REVOLUTION

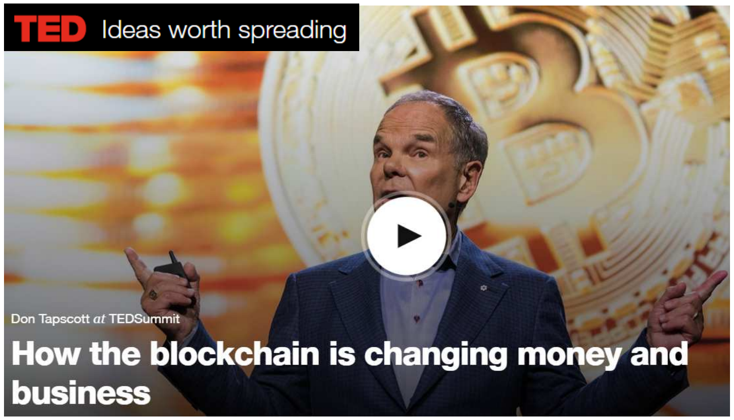
HOW THE TECHNOLOGY BEHIND BITCOIN IS CHANGING MONEY, BUSINESS, AND THE WORLD

DON TAPSCOTT

BESTSELLING AUTHOR OF *WIKINOMICS*

and ALEX TAPSCOTT

Copyrighted Material



Don Tapscott *at* TEDSummit

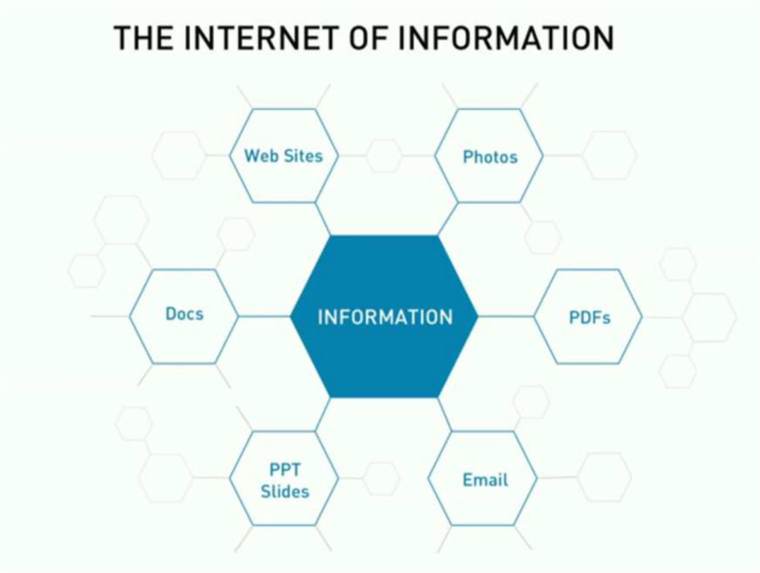
How the blockchain is changing money and business

Blockchain Definition

- A blockchain is a **decentralized database** and **a peer-to-peer network** that stored a **registry of transactions**.
- It is a type of **distributed public ledger** that keeps **continuously updated** digital records of **who owns what**.

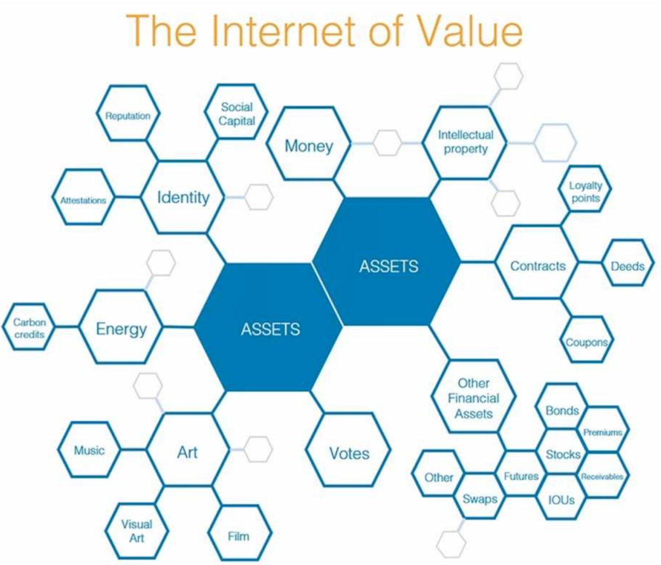
From the internet of information to the internet of value

- “The blockchain is the second significant overlay on the internet, just as the web was the first layer back in 1990. It is advancing like a tsunami, enveloping everything along its way.” -- William Mougayar



“Blockchain is the internet of value.”

-Don Tapscott, technology author



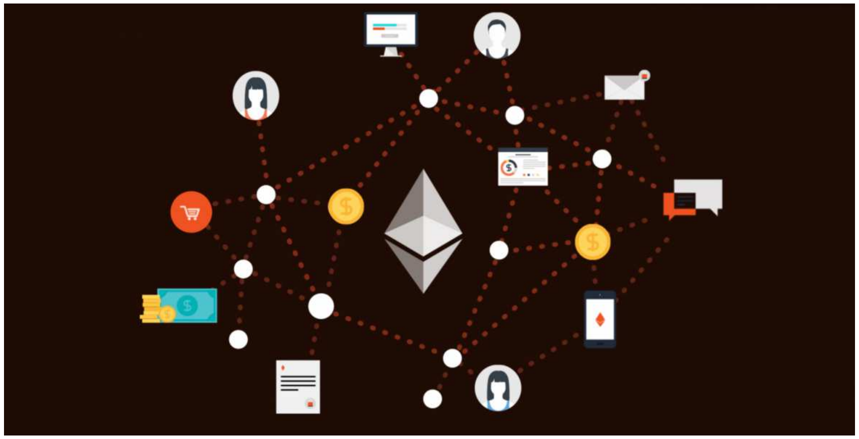
Blockchain Application

"**Blockchain is to Bitcoin, what the internet is to email.** A big electronic system, on top of which you can build applications. Currency is just one." — **Sally Davies, FT Technology Reporter**

The best example of the evolution and broad application of blockchain, beyond digital currency, is the development of the **Ethereum public blockchain**, which is providing a way to execute peer to peer **Smart Contracts**.

Ethereum / Smart Contract

Ethereum: an open-source, public, blockchain-based distributed computing platform featuring **smart contract** (programming) functionality. It provides a decentralized **Turing-complete** virtual machine, the **Ethereum Virtual Machine** (EVM), which can execute scripts using an international network of public nodes.



What are blockchains good at

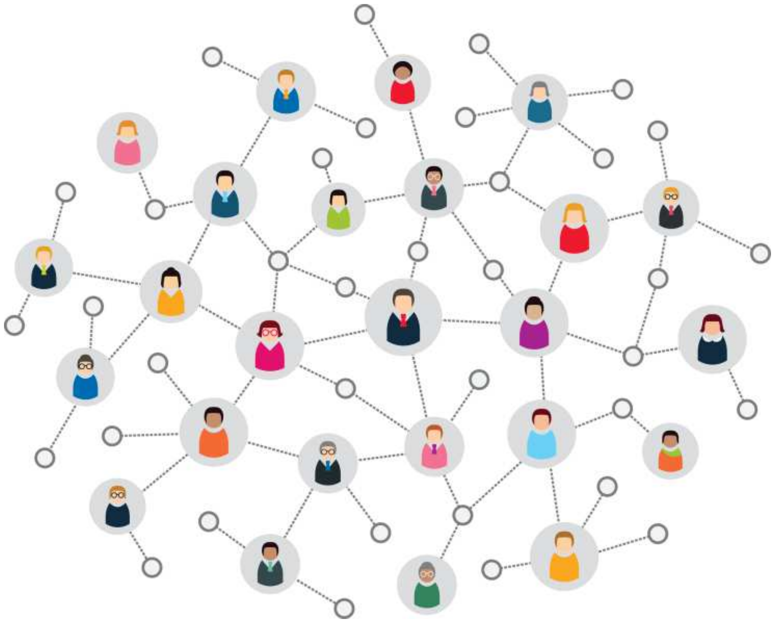
- **Adjudicating Trust** – in the exchange of value, whatever that value may be, with blockchain the participants don't need to trust each other. **They trust the "math" behind the blockchain platform.**
- **Transactions** – **blockchains are optimized to facilitate transactions** between parties, whether it is exchange of value, data, etc.
- **Incentivized Participation** – "Game Theory". The participants in the blockchain are rewarded as a result of their participation,
- **Transparency** – the ledger is an open book – anyone can see the transaction history and trace data through the blockchain.
- **Accountability** – like transparency, it is easy to account for every transaction on the blockchain and independently verify it.
- **Immutability** – Once a transaction has been recorded in the blockchain, it is written in "digital stone."

Blockchain Technology to Boost Cyber Security

- **Blockchain provides a fundamentally different approach to cybersecurity**
- **No single point of failure**
- **Preventing fraud and data theft**
- **Using blockchain technology to safeguard data (Guardtime)**
- **Using blockchain to prevent Distributed Denial of Service (DDoS) attacks**

Protecting Identities

- By combining the decentralized blockchain principle with identity verification, a **digital ID** can be created to act as a digital watermark which can be assigned to every online transaction of any asset.
- There are more than 20 pioneers competing in building blockchain-based identity management and authentication solutions for cross-industry applications.



Preventing data theft in untrusted environments

- Encrypting data has now become a norm across organizations
- However, when you want to act upon that data, you’ll have to decrypt and reveal its contents
- Currently, there’s really no option for computing over encrypted data in the market
- There are many situations where we want to jointly work on data without revealing our portion to untrusted entities

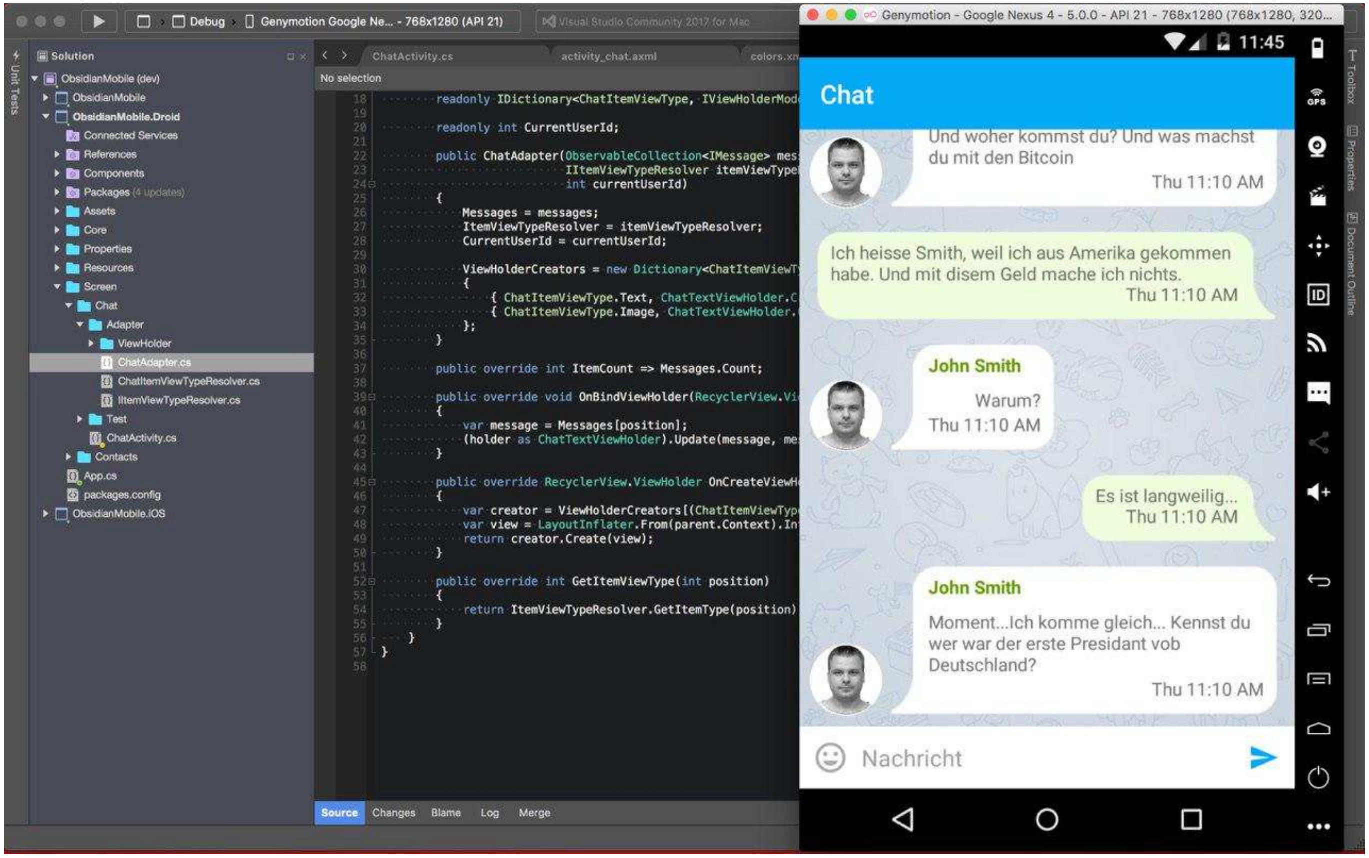
Why Passwords are the New Exploits

- Yahoo hack: 1bn accounts compromised by biggest data breach in history. Twitter 33 million. LinkedIn 165 million. Myspace 360 million, Dropbox hack leads to leaking of 68m user passwords on the internet
- There are now over a billion owned accounts with credentials sold online.
- Hackers nab $500,000 as Enigma is compromised weeks before its ICO
- https://haveibeenpwned.com/

Making Passwords Obsolete

- No more passwords — no more break-ins.
- Blockchain powered Access Management solution, replacing passwords with the distributed authentication.

Ensures the Privacy and Security of Chats



```
        readonly IDictionary<ChatItemViewType, IViewHolderMod

        readonly int CurrentUserId;

        public ChatAdapter(ObservableCollection<IMessage> mes
                           IItemViewTypeResolver itemViewType
                           int currentUserId)
        {
            Messages = messages;
            ItemViewTypeResolver = itemViewTypeResolver;
            CurrentUserId = currentUserId;

            ViewHolderCreators = new Dictionary<ChatItemViewTy
            {
                { ChatItemViewType.Text, ChatTextViewHolder.C
                { ChatItemViewType.Image, ChatTextViewHolder.
            };
        }

        public override int ItemCount => Messages.Count;

        public override void OnBindViewHolder(RecyclerView.Vi
        {
            var message = Messages[position];
            (holder as ChatTextViewHolder).Update(message, me
        }

        public override RecyclerView.ViewHolder OnCreateViewH
        {
            var creator = ViewHolderCreators[(ChatItemViewTyp
            var view = LayoutInflater.From(parent.Context).In
            return creator.Create(view);
        }

        public override int GetItemViewType(int position)
        {
            return ItemViewTypeResolver.GetItemType(position)
        }
    }
}
```

Und woher kommst du? Und was machst du mit den Bitcoin
Thu 11:10 AM

Ich heisse Smith, weil ich aus Amerika gekommen habe. Und mit disem Geld mache ich nichts.
Thu 11:10 AM

John Smith
Warum?
Thu 11:10 AM

Es ist langweilig...
Thu 11:10 AM

John Smith
Moment...Ich komme gleich... Kennst du wer war der erste Presidant vob Deutschland?
Thu 11:10 AM

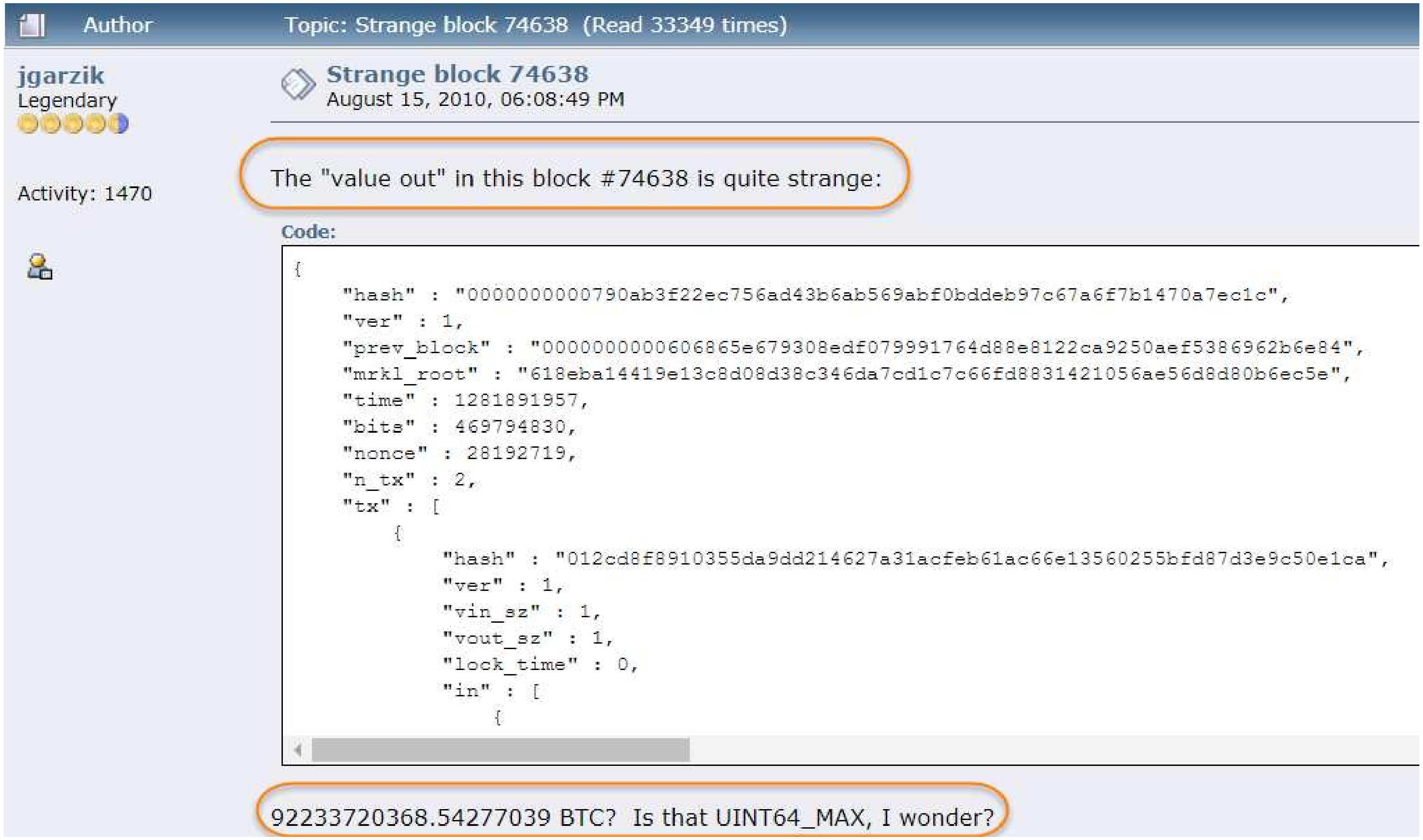
The future looks bright for blockchain-based security platforms

- The blockchain addresses the fundamental flaws of security by taking away the human factor from the equation, which is usually the weakest link. By leveraging a distributed ledger and taking away the risk of a single point of failure, blockchain technology provides end-to-end privacy and encryption while still ensuring convenience for users.
- Bitcoin and its underlying blockchain have proved to be resilient, and the numerous new blockchain technologies offer even more promise in terms of extensibility and robustness, especially in the field of security.

Bitcoin Integer Overflow Incident

- On **8th August 2010** bitcoin developer Jeff Garzik wrote what could be mildly described as the biggest understatement since Apollo 13 told Houston: "We've had a problem here.“
- “***The ‘value out’ in this block is quite strange***,” he wrote on bitcointalk.org, referring to a block that had somehow contained **92 billion** BTC, which is precisely 91,979,000,000 more bitcoin than is ever supposed to exist (max supply 21m).
- The bug is known as a **integer overflow** error. Some hacker found a way to flood the code and create a ridiculously large amount of bitcoin in the process.
- The fix was the bitcoin equivalent of dying in a video game and restarting from the last save point: rollback 24 hours.

The 'value out' in this block is quite strange:



Author | Topic: Strange block 74638 (Read 33349 times)

jgarzik
Legendary

Activity: 1470

Strange block 74638
August 15, 2010, 06:08:49 PM

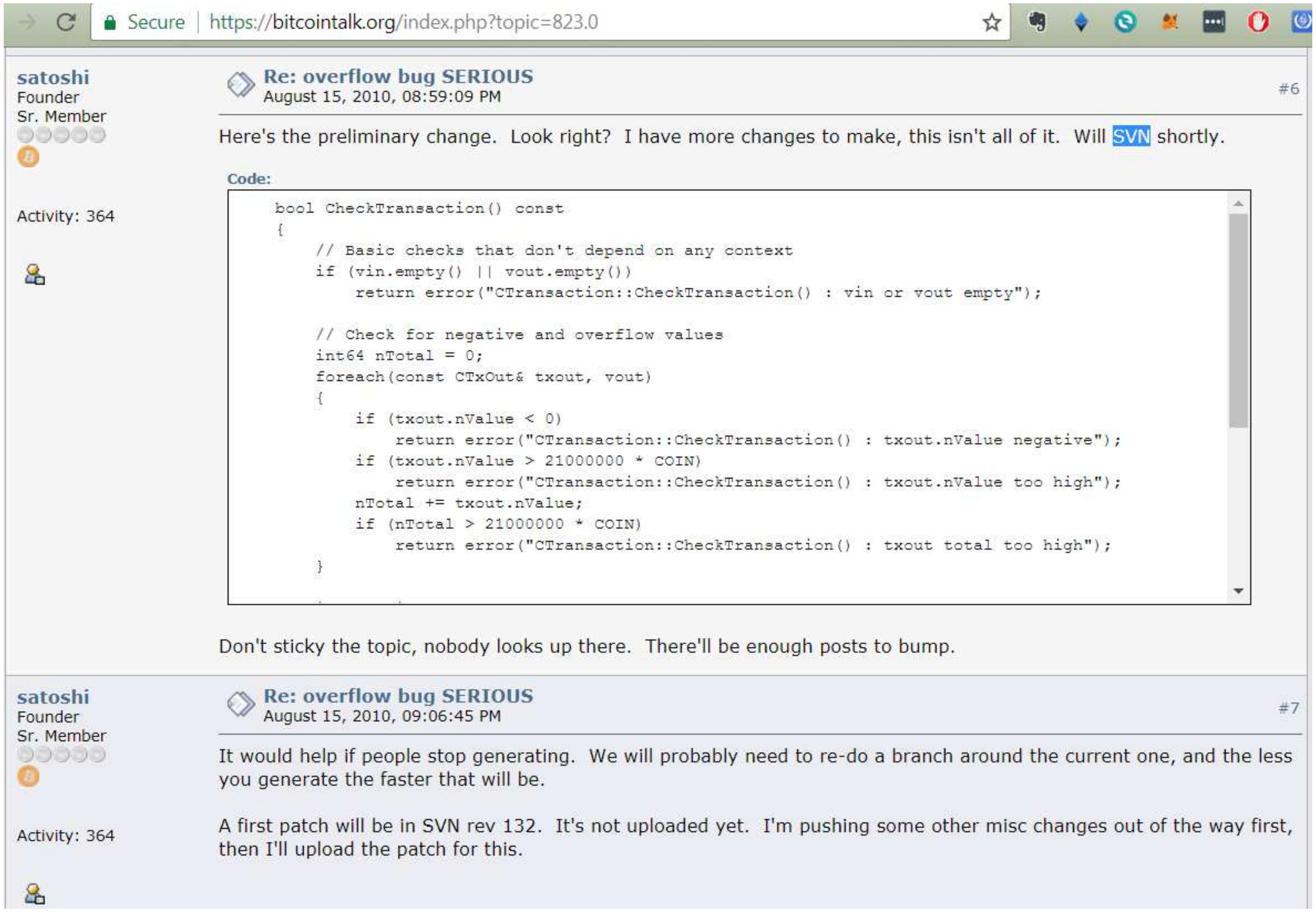
The "value out" in this block #74638 is quite strange:

Code:

```
{
    "hash" : "0000000000790ab3f22ec756ad43b6ab569abf0bddeb97c67a6f7b1470a7ec1c",
    "ver" : 1,
    "prev_block" : "0000000000606865e679308edf079991764d88e8122ca9250aef5386962b6e84",
    "mrkl_root" : "618eba14419e13c8d08d38c346da7cd1c7c66fd8831421056ae56d8d80b6ec5e",
    "time" : 1281891957,
    "bits" : 469794830,
    "nonce" : 28192719,
    "n_tx" : 2,
    "tx" : [
        {
            "hash" : "012cd8f8910355da9dd214627a31acfeb61ac66e13560255bfd87d3e9c50e1ca",
            "ver" : 1,
            "vin_sz" : 1,
            "vout_sz" : 1,
            "lock_time" : 0,
            "in" : [
                {
```

92233720368.54277039 BTC? Is that UINT64_MAX, I wonder?

Satoshi’s Patch within 5 hours



satoshi
Founder
Sr. Member

Activity: 364

Re: overflow bug SERIOUS
August 15, 2010, 08:59:09 PM
#6

Here's the preliminary change. Look right? I have more changes to make, this isn't all of it. Will SVN shortly.

Code:

```
    bool CheckTransaction() const
    {
        // Basic checks that don't depend on any context
        if (vin.empty() || vout.empty())
            return error("CTransaction::CheckTransaction() : vin or vout empty");

        // Check for negative and overflow values
        int64 nTotal = 0;
        foreach(const CTxOut& txout, vout)
        {
            if (txout.nValue < 0)
                return error("CTransaction::CheckTransaction() : txout.nValue negative");
            if (txout.nValue > 21000000 * COIN)
                return error("CTransaction::CheckTransaction() : txout.nValue too high");
            nTotal += txout.nValue;
            if (nTotal > 21000000 * COIN)
                return error("CTransaction::CheckTransaction() : txout total too high");
        }
```

Don't sticky the topic, nobody looks up there. There'll be enough posts to bump.

satoshi
Founder
Sr. Member

Activity: 364

Re: overflow bug SERIOUS
August 15, 2010, 09:06:45 PM
#7

It would help if people stop generating. We will probably need to re-do a branch around the current one, and the less you generate the faster that will be.

A first patch will be in SVN rev 132. It's not uploaded yet. I'm pushing some other misc changes out of the way first, then I'll upload the patch for this.

Estonia National ID Security Flaw

- If you want a glimpse at the future potential of blockchain, visit Estonia.
- In Estonia, this distributed ledger (blockchain technology) gives citizens and residents more control over their own data.
- Estonia freezes resident ID cards due to security flaw (https://www.engadget.com/2017/11/04/estonia-freezes-resident-id-cards-security-flaw/)

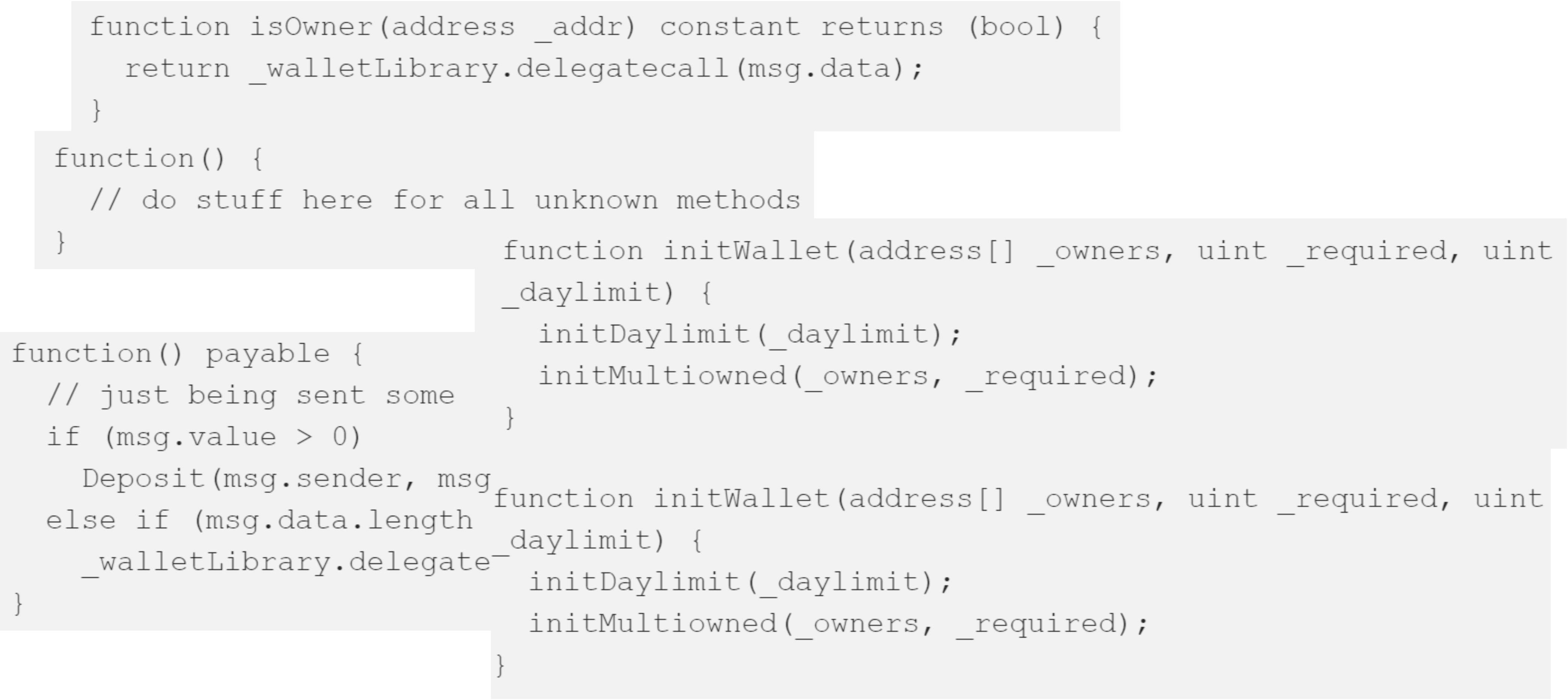
The DAO Attack on Ethereum

- The DAO ICO launched on 30th April, 2016
- The DAO was popular, raising over $150m
- **17th June**, an attacker managed to drain more than 3.6 million Ether into a “child DAO” that has the same structure as The DAO. **Code Issue Leads to $60 Million Ether Theft**
- Soft Fork Proposal / Hard Fork Proposal
- Ethereum was hard forked on 20th July 2016. Ethereum Classic was born

Multisig Wallet Hack

- **19th June 2017**: an unknown hacker exploited a critical flaw in the Parity multi-signature wallet on the Ethereum network, draining three massive wallets of over $31m worth of Ether in a matter of **minutes**. Given a couple more hours, the hacker could've made off with over $180m 0 from vulnerable wallets.
- A group of white-hat hackers from the Ethereum community rapidly organized: **hack the remaining wallets before the attacker did**

Look inside



```
function isOwner(address _addr) constant returns (bool) {
  return _walletLibrary.delegatecall(msg.data);
}
```

```
function() {
  // do stuff here for all unknown methods
}
```

```
function initWallet(address[] _owners, uint _required, uint
_daylimit) {
  initDaylimit(_daylimit);
  initMultiowned(_owners, _required);
}
```

```
function() payable {
  // just being sent some
  if (msg.value > 0)
    Deposit(msg.sender, msg
  else if (msg.data.length
    _walletLibrary.delegate
}
```

```
function initWallet(address[] _owners, uint _required, uint
_daylimit) {
  initDaylimit(_daylimit);
  initMultiowned(_owners, _required);
}
```

The future: Cyber Security more important than ever

- This attack is important. It shakes people up. It forces the community to take a long, hard look at **security best practices**. It forces developers to treat **smart contract programming** with far more rigor than they currently do.
- https://consensys.github.io/smart-contract-best-practices/
- Story like this gets us closer to really deeply understanding the technology of blockchain — both its dangers, and its amazing potential.