Bitcoin, Blockchain and Beyond...

Satish Babu
Chair, ISOC-TRV
Chair, APRALO/ICANN

Overview

- What's a (Digital) Currency ?
- Bitcoin: Revolutionary ?
- The Blockchain
- Ethereum and recent developments
- The Future

What is a (Digital) Currency?

Currencies, Trust and Confidence

- The value of a currency is based on:
  - The trust that users have in the currency
  - The percieved utility of the currency
- The value is not always based on the actual worth of the coin
- In other words, currency is a ‘token’ of a consensus decision
- Digital currencies and many other private currencies are also tokens

Trusted Intermediaries

- We are used to dealing with ordinary currency, which is technically called **fiat currency**
- Fiat currencies require a **trusted intermediary** such as the Government or Banks to facilitate and guarantee transactions
- Because of the intermediary, digital transactions are always traceable (unlike cash transactions)
- Intermediaries are able to stop transactions and freeze accounts of individuals or institutions
- Sometimes trusted intermediaries abuse the trust of others (or get hacked)

Bitcoin: Revolutionary?

**“We reject kings, presidents and voting.
We believe in rough consensus and running code.”**

— Internet Engineering Task Force (IETF)

“...[with cryptography] no amount of violence will ever solve a math problem.”

— Jacob Appelbaum, Cypherpunks:
Freedom and the Future of the Internet

Bitcoin, the original Cryptocurrency

- A paper entitled “Bitcoin: A Peer-to-peer Electronic Cash System” appeared on the Internet towards the end of 2008
- The paper had an end-to-end description of a community-controlled digital currency
- It turned out that the author of the paper, Satoshi Nakamoto, was fictional
- The associated domain, bitcoin.org, was registered anonymously in Aug 2008

Bitcoin: Design objectives

- Create a Digital Currency that:
  - Would enable **direct transfer of value** between two entities unknown to each other (except by their addresses) over the Internet
  - Would not require any third party as a “Trusted Intermediary” for any purpose (eg., as book-keeper or transaction validator)
  - Assumes that the network has a significant number of malicious/dishonest nodes (who provide wrong info, “hack” records, spend a coin that is already spent etc)

Bitcoin Properties

Bitcoin, according to the original definition:

- Is a currency based on cryptography
- Is meant to make payments and financial transfers
- Assumes that the network has malicious actors but these are less than the majority (in terms of computing power)
- Addresses the double-spending problem
- Maintains decentralized, tamper-proof community accounts, through consensus process based on **“proof-of-work”**
- Provides for parties to be protected by pseudoanonymous identities
- Allows nodes to join and leave at will

Bitcoin: What's innovative?

- No central controller, no master node…
- Easy to transfer, secure, verify, granulate
- Predictable, limited in supply
- Not backed by gold or debt, but by perceived value
- Has (weak) anonymity for parties
- Freeze-proof: Third party cannot block transactions
- Faster and cheaper than fiat currency
- Integrity protected by cryptography

Bitcoin: What can you do with it?

- Transfer bitcoin currency (BTC) to another party identifed by their address
- Receive BTC into an address from another party
- Create any number of new addresses to receive funds
- Create a multiparty (“MultiSig”) transaction (eg., 2 out of 3 parties can approve)
- Create escrows through MultiSig

Bitcoin: What does the Network do?

- Ensure that the network is open for everyone to enter/exit
- Ensure that transactions are validated and placed into blocks in a reasonable time through consensus (“mining”) and confirm transactions
- Dynamically calibrate the proof-of-work mechanism to ensure blocks are mined in a reasonable time
- Reward the miner who puts together a valid block with new bitoins (12.5 BTC right now)

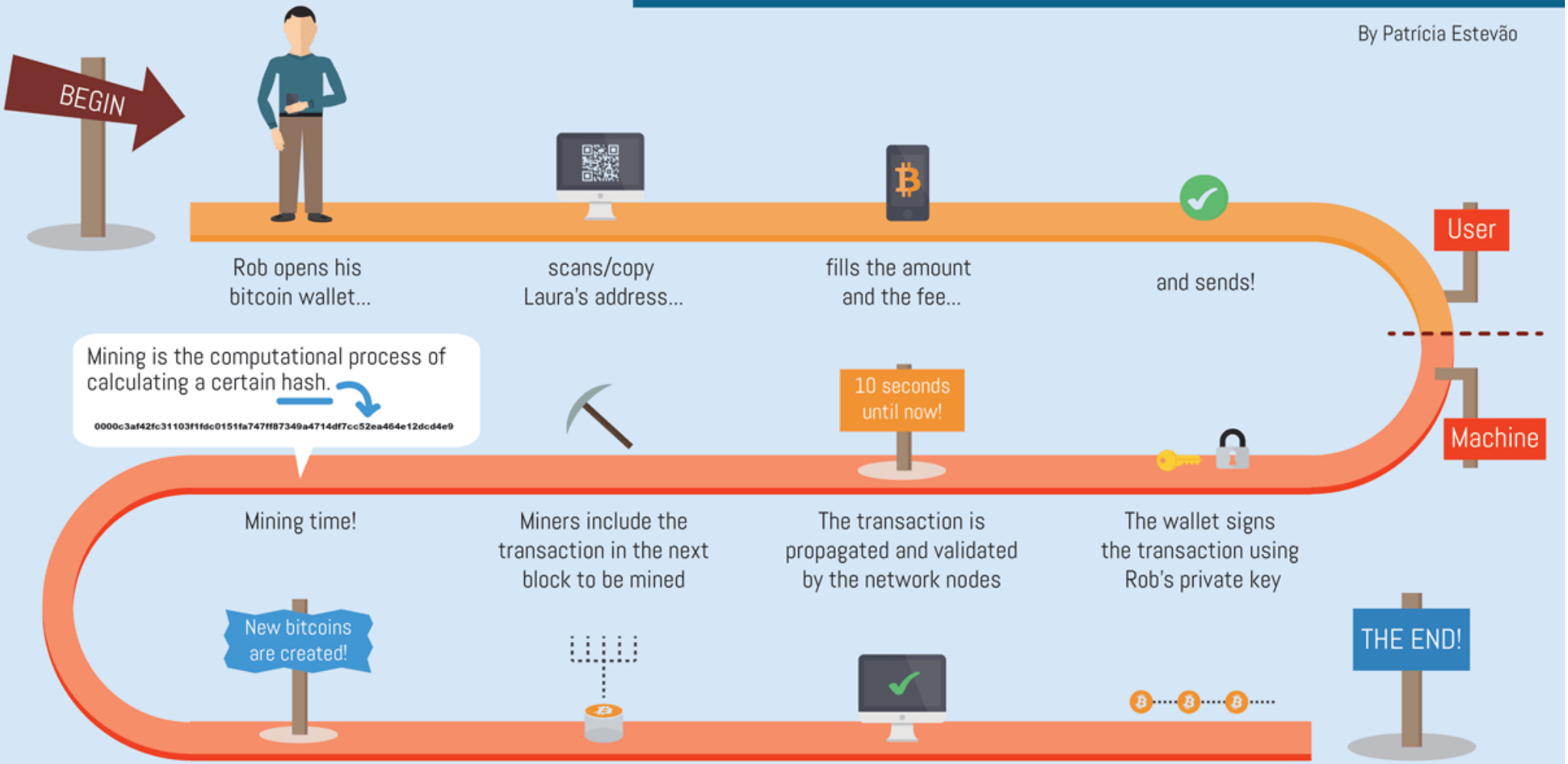
Bitcoin Exchanges

- Bitcoin Exchanges do the following tasks:
  - Convert between Fiat Currency and BTC/BCC (and other cryptocurrencies)
  - Provide user wallets
  - Report to Government and LEA
  - Provide Escrow and other financial services
  - Charge transaction fees to support themselves

THE BITCOIN TRANSACTION LIFE CYCLE

Rob's quest to send 0.3 BTC to his friend Laura

By Patrícia Estevão



Bitcoin facts

- Global currency that’s not controlled by any Government
- A person’s wallet contains private keys only...duplicating it does not double the money
- If wallets are lost, coins are irretreivable
- Transactions cannot be reversed. Escrow is possible
- Anyone with computing power more than 50% global computing power can take over the currency

Bitcoin today

- From its initial price levels (in 2010, a $25 pizza costed 10,000 BTC), BTC crossed $5800 in Oct ‘17
- The total market capitalization of BTC is about $95 billion (Oct 2017)
- As of today, the bitcoin protocol has not been hacked even once (although lots of BTC have been lost) and the chain has forked a couple of times
- Some consider Bitcoin to be a high-return investment (but it’s also high risk, and legally in a grey area)

Bitcoin in Summary

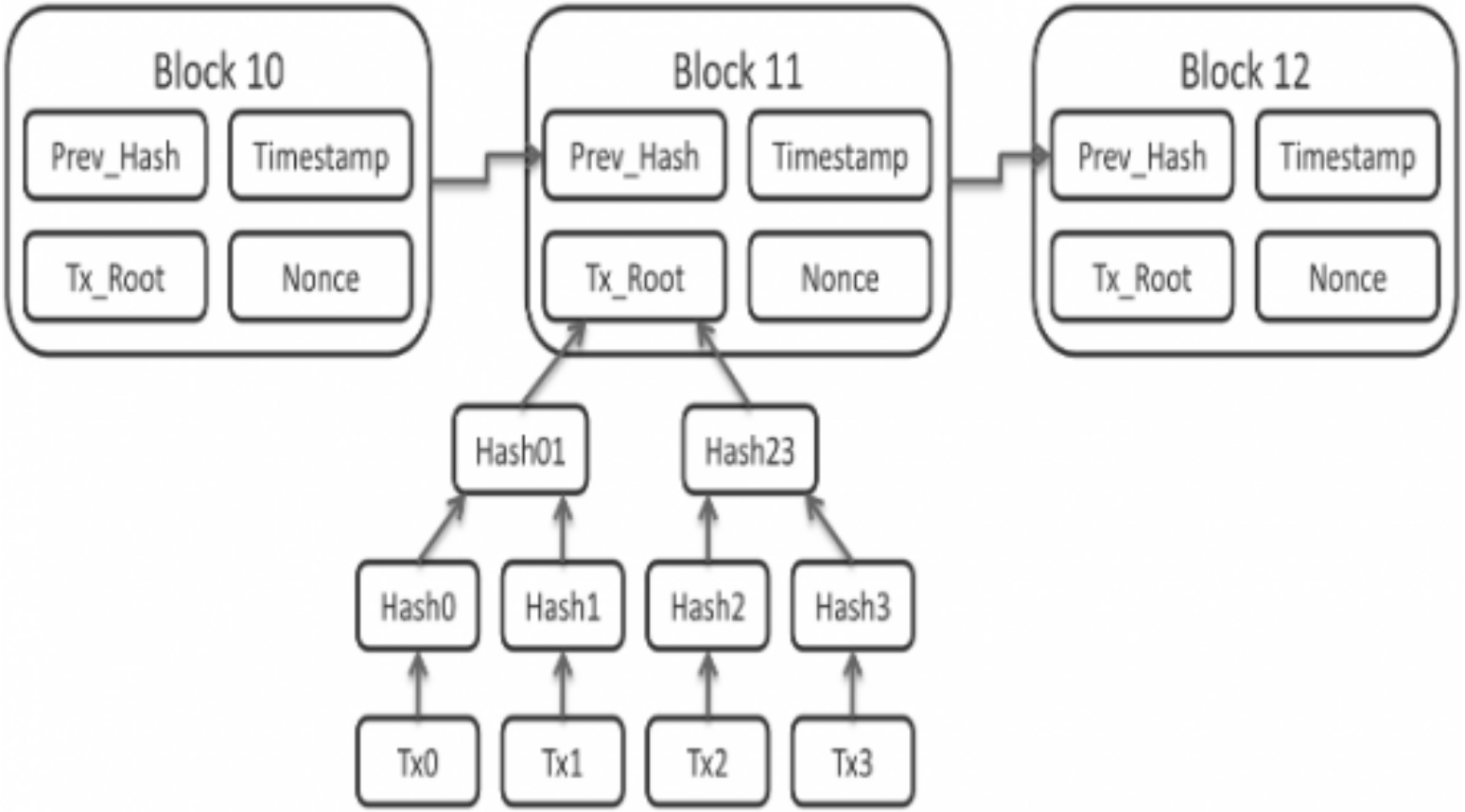
- The revolutionary aspect of Bitcoin is not that it is a universal digital currency, nor that it is easy to use
- **The Bitcoin has brought in a Revolution in Trust**, where we do not need Governments or other ‘trusted’ central authorities to transact or even to store critical information
- In the Bitcoin system, it is the **Blockchain** that implements the important property of immutable storage

The Blockchain: The Internet of Truth?

“Anybody can put something up on the Internet. It’s harder and harder to find out what the truth is.”

— Robert Redford

Blockchain: Simplified Structure



What is unique about the Blockchain?

- Unlike a database that can be hacked into by malicious entities, a blockchain cannot be modified once written, because:
  - Many identical copies of the blockchain exist
  - Blockchains are append-only. If an earlier block is modified, all the subsequent blocks instantly become invalid & need to be rebuilt
  - Insertion of incorrect data into a block by a malicious node will cause it to be rejected by the rest of the nodes
  - All this is done without any “trusted” central authority

The Post-Bitcoin Scenario

“Code is Law”

— Lawrence Lessig, Harvard Law School

After the Bitcoin

- The success of bitcoin and its limitations (for instance, long confirmation times and the absence of a Turing-complete scripting language) spawned a large number of ‘Altcoins’
- Many of these were currency (Litecoin, Dogecoin), or special purpose (NameCoin)
- Gradually, people began to feel the need for a blockchain-based generic computing platform

Ethereum

- The first of these generic blockchain-based platforms is Ethereum:
  - A Blockchain-based global computer with numerous nodes with no entry barriers
  - Has a Turing-complete embedded programming language
  - Has two kinds of accounts: (a) User accounts; (b) Contracts
  - Contracts are applications (or blocks of code) that can execute autonomously
  - The state of the entire Ethereum ecosystem is stored in the Blockchain

Ethereum (2)

- In effect, Ethereum is a global, secure, blockchain-based computer that:
  - Has its own blockchain that can be used to store user accounts or contracts

  Has its own currency, “Ether” Ξ, for storing/transacting value
  - Can store and execute Smart Contracts which are code blocks
  - Every node stores the full blockchain
  - Contracts can call other contracts or transfer currency
  - Uses “gas” (fees) to impose execution/storage limits

Ethereum Innovations

- Multiple Digital Currencies: Ethereum makes it easy to issue custom digital currencies
- Smart Contracts: Ethereum’s blockchain can hold transactions as well as code, which enables creation of smart contracts that are triggered by conditions
- Smart Property: Property can be represented as smart tokens which can be traded & transacted
- Decentralized Autonomous Organizations (DAOs): All the above combined, together with protocols, to make a self-governing, self-executing organization

Non-Financial Use Cases

Digital Content/Documents, Storage & Delivery

BitProof, Blockcai, Ascribe, ArtPlus, Chainy.Link, Stampery, Blocktech (Alexandria), Bisantyum, Blockparti, The Rudimental, BlockCDN

Authentication & Authorization

The Real McCoy, Degree of Trust, Everpass, BlockVerify,

Digital Identity

Sho Card, Uniquid, Onename, Trustatom

Marketplace

Providing premium rights & brand based coins: MyPowers

Smart Contracts

Otonomos, Mirror, Symbiont, New system Technologies

Real Estate

Factom

Diamonds

Everledger

Gold & Silver

BitShares, Real Asset Co., DigitalTangible (Serica), Bit Reserve

Reviews/Endorsement

TRST.im, Asimov (recruitment services), The World Table

Blockchain in IoT

Filament, Chimera-inc.io, ken Code – ePlug

App Development

Proof of ownership for modules in app development: Assembly

Network Infrastructure & APIs

Ethereum, Eris, Codius, NXT, Namecoin, Colored Coins, Hello Block, Counterparty, Mastercoin, Corona, Chromaway, BlockCypher

Other

Prediction platform: Augur
Election Voting: Follow My Vote
Patient Records management: BitHealth

Financial Use Cases

Currency Exchange & Remittance

Coinbase (Wallet), BitPesa, Billion, Ripple, Stellar, Kraken, Fundrs.org, MeXBT, CryptoSigma

P2P Transfers

BTC Jam, Codius, BitBond, BitnPlay (Donation), DeBuNe (SME's B2B transactions)

Ride Sharing

La'zooz

Data Storage

Storj.io, Peernova

Trading Platforms

equityBits, Spritzle, Secure Assets, Coins-e, DXMarkets, MUNA, Kraken, BitShares

Gaming

PlayCoin, Play(on DACx platform), Deckbound

Ethereum Use Cases

- Verifiable Electronic voting
- Community-owned databases (eg., farmers, consumers)
- E-Tendering
- Internet of Things (IoT)
- Online medical records
- Land records
- Digital document management

Technical aspects of Ethereum

- Ethereum runs as the **Ethereum Virtual Machine**, a single, global, machine
- The minimum SDK consists of Ethereum CLI
- The main programming language is **Solidity**, which runs on several popular IDEs
- Apps on the platform are called **ĐApps** (Decentralized Applications). DApp backends run on the EVM and front-end could be on **Swarm** or **IPFS**

Conclusions

The Future

- Bitcoin was the first-ever cryptocurrency, and seen as a remarkable development
- The Blockchain, at the heart of Bitcoin, was considered as a disruptive development that had numerous applications
- Ethereum, with a full programming environment, is seen as a second-generation crypto platform that will have numerous general-purpose applications

Thank you!