THE ZCASH FOUNDATION

A non-for-profit organization , serving the Zcash community and promoting financial privacy

INTRODUCTION

Oyedeji Oluwoye

- Nigeria Origin
- Network Planning Engineer
- Global Implementation Team
- Cisco certified wireless Design and IP Networking
- CS BS Alabama A&M University
- CS MS Alabama A&M University
- Thesis ”The Network Analysis of Bitcoin & Cryptocurrency”
- Founder of Concentrix Capital
- Board member of Lamden

THE ORIGIN

Who created this technology

Satoshi Nakamoto

bitcoin White Paper

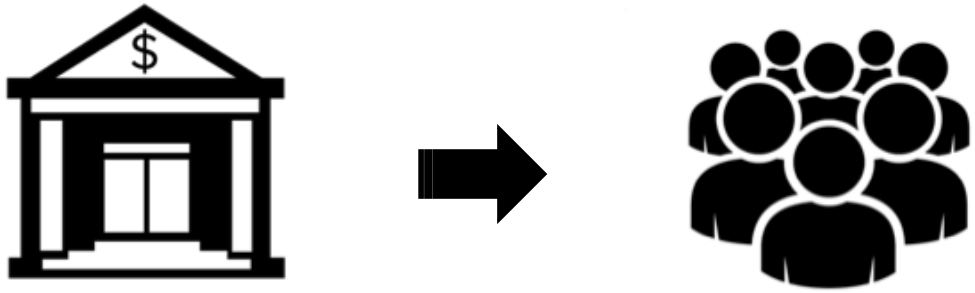
bitcoin

Bitcoin

Altcoins

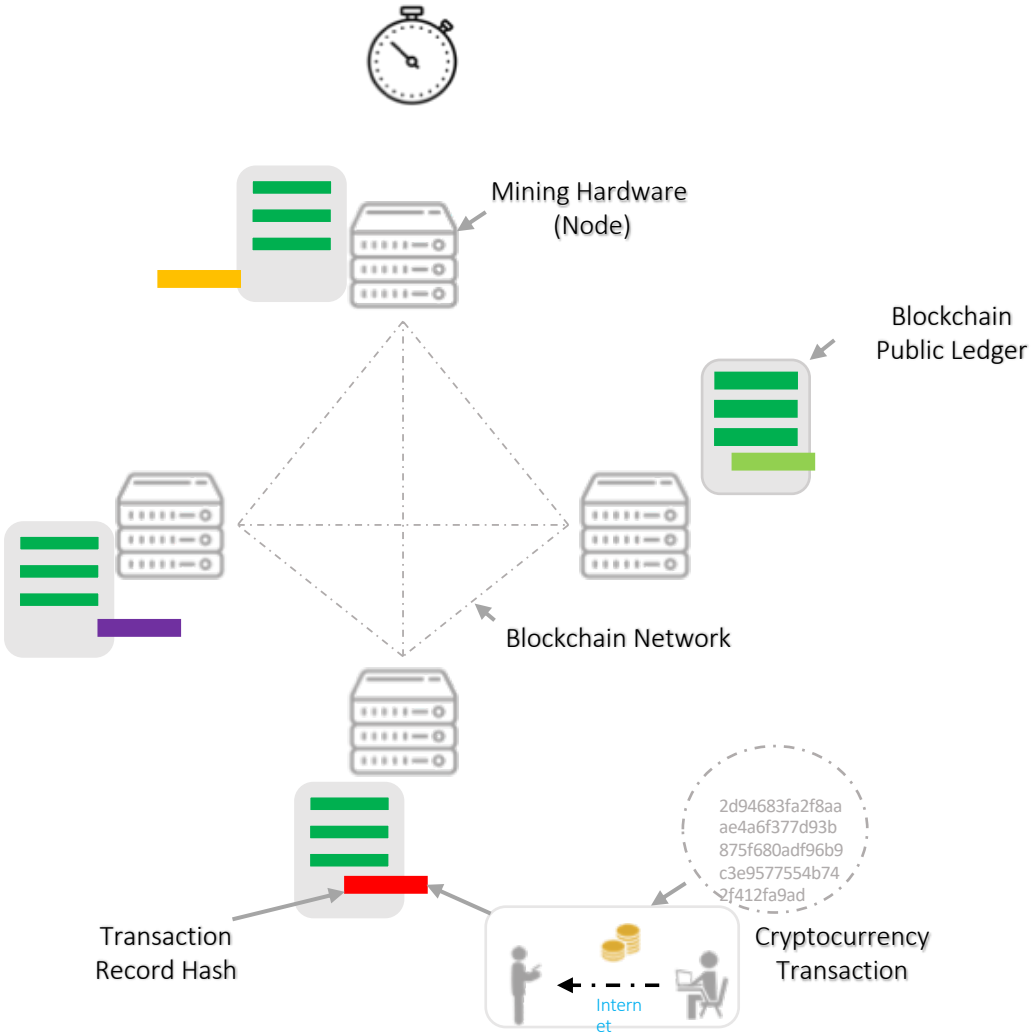
Why did they create this technology

2008 US Housemaker Crash

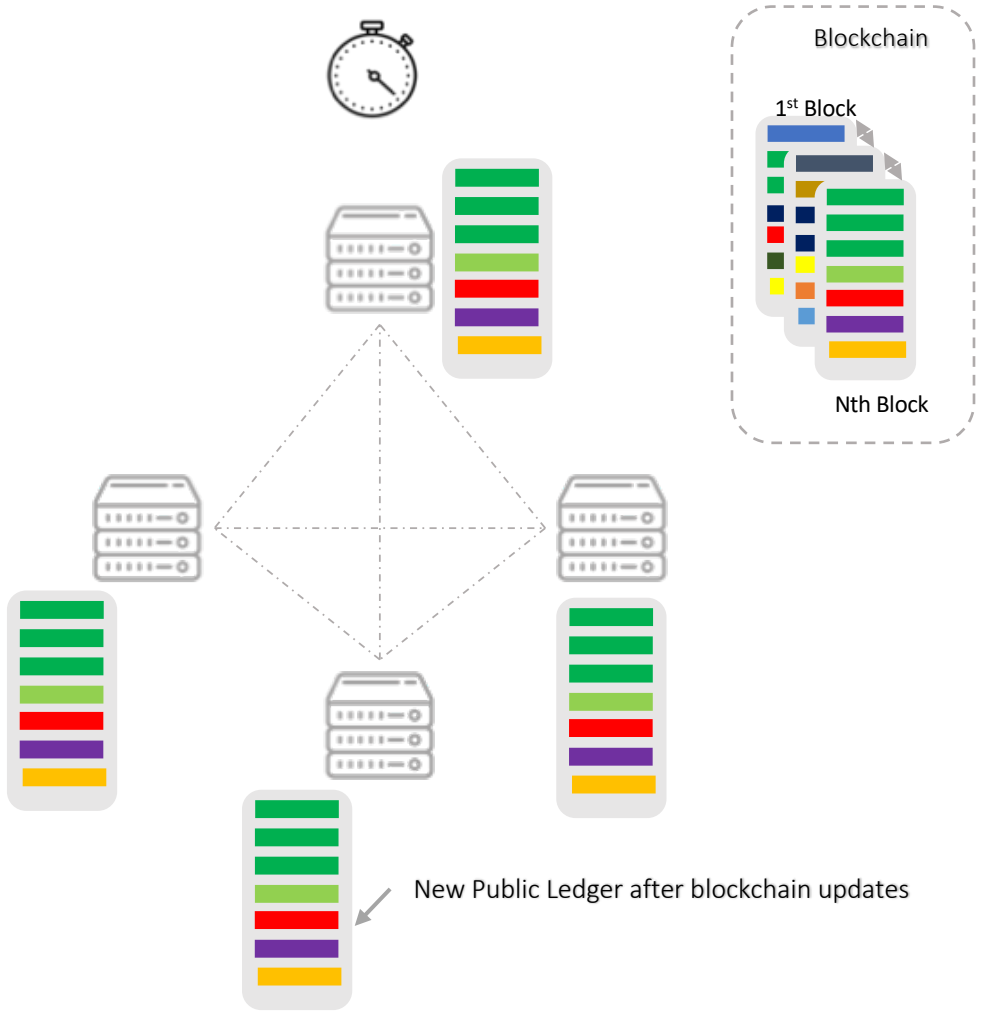


Handing financial power to the people

HOW IT WORKS

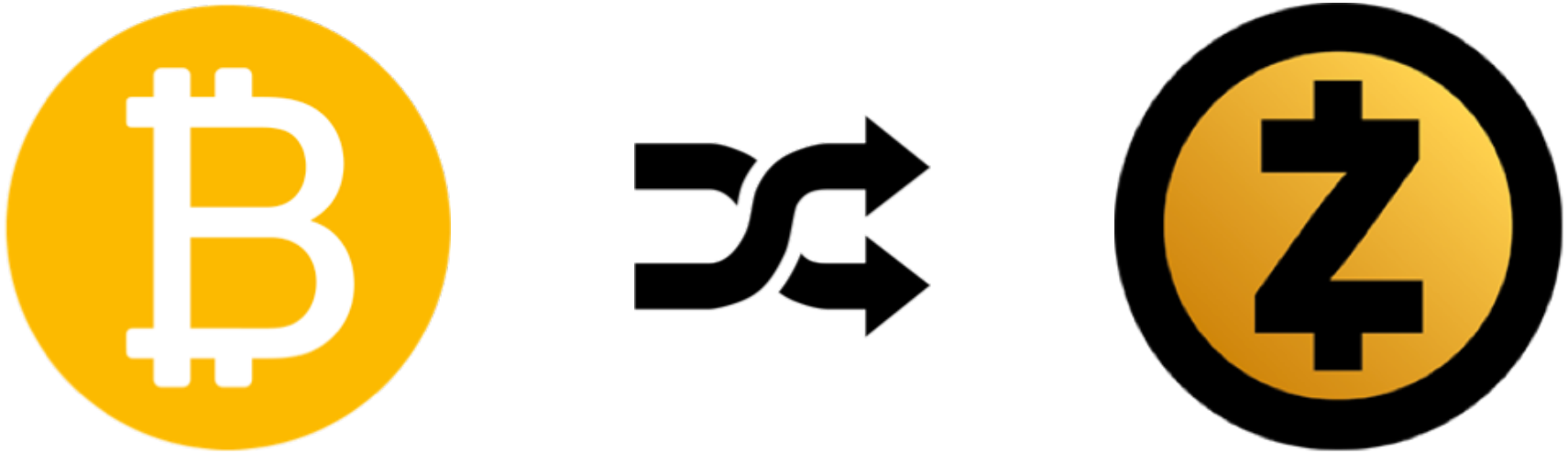


During Blockchain Transactions



After Blockchain Public Ledger Update

ZCASH ORIGIN



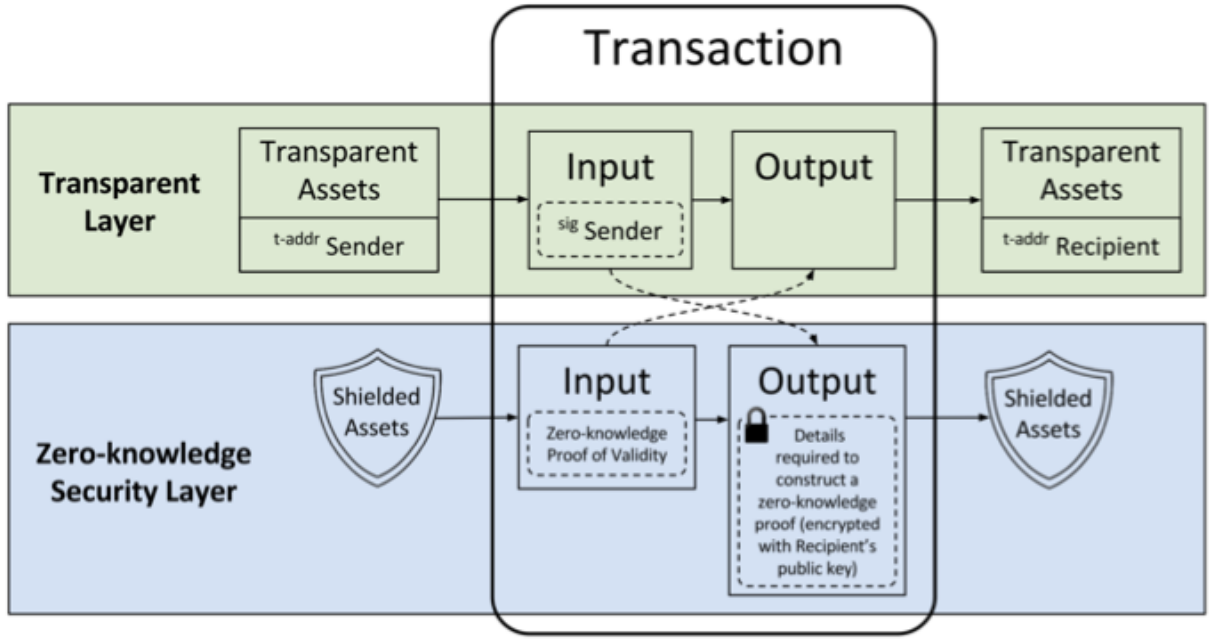
Zcash is a decentralized peer-to-peer cryptocurrency. It was created as a fork of Bitcoin and quite like bitcoin it also has a hard limit of 21 million coins. But that is where the comparison ends. Unlike bitcoin, Zcash offers complete and total privacy for their users through the use of some ingenious cryptography.

"Zcash is the first open, permission-less cryptocurrency that can fully protect the privacy of transactions using zero-knowledge cryptography."- **Zcash website**

ZCASH vs bitcoin

	bitcoin (btc)	**zcash (zec)**
concept	digital money	private digital money
transaction details	publicly viewable	concealed from public
transaction example	address x sent 1 btc to address y	? sent ? zec to ?
market cap (as of dec 2017)	~$235 billion	~$900 million
release date	jan 2009	oct 2016
release method	mining	mining w/ founders' reward

Zk-SNACKS



Zcash uses a specific cutting edge form of zero knowledge verification called zk-SNACKs zero knowledge succinct non-interactive arguments of knowledge).

Zcash allows for public and private transactions with the option for the user to selectively disclose information about their private transactions. Optional transparency can be beneficial for situations where an entity needs to be audited or submit information for tax purposes.

ZCASH IMPLEMENTATION

Zcash is a cryptocurrency launched by Zerocoin Electic Coin Company on 9th September 2016 and is the first example a cryptocurrency marrying the concepts of blockchain technology with Zk-Snarks
Ethereum wants to integrate Zk-Snarks as it enters its Metropolis phase and the way that they are planning to do so is by creating an alliance with Zcash which will include a mutual exchange of value.

The development firm behind the privacy-focused public blockchain zcash has announced the first integration of its zero-knowledge security layer (ZSL) into an enterprise blockchain, with JPMorgan today revealing it has added the functionality to its Quorum blockchain.