THE ZCASH FOUNDATION

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

- 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

Oyedeji Oluwoye
THE ORIGIN

Who created this technology

Satoshi Nakamoto

Why did they create this technology

2008 US Housemaker Crash

Handing financial power to the people
**HOW IT WORKS**

**During Blockchain Transactions**

- **Mining Hardware (Node)**
- **Blockchain Public Ledger**
- **Blockchain Network**
- **Transaction Record Hash**
- **Cryptocurrency Transaction**

**After Blockchain Public Ledger Update**

- **Blockchain**
- **1st Block**
- **Nth Block**
- **New Public Ledger after blockchain updates**
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

<table>
<thead>
<tr>
<th></th>
<th>bitcoin (btc)</th>
<th>zcash (zec)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>concept</strong></td>
<td>digital money</td>
<td>private digital money</td>
</tr>
<tr>
<td><strong>transaction details</strong></td>
<td>publicly viewable</td>
<td>concealed from public</td>
</tr>
<tr>
<td><strong>transaction example</strong></td>
<td>address x sent 1 btc to address y</td>
<td>? sent ? zec to ?</td>
</tr>
<tr>
<td><strong>market cap (as of dec 2017)</strong></td>
<td>~$235 billion</td>
<td>~$900 million</td>
</tr>
<tr>
<td><strong>release date</strong></td>
<td>jan 2009</td>
<td>oct 2016</td>
</tr>
<tr>
<td><strong>release method</strong></td>
<td>mining</td>
<td>mining w/ founders’ reward</td>
</tr>
</tbody>
</table>
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 is a cryptocurrency launched by Zerocoin Electric 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.