

***Blockchain: The Information Technology of the Future***  
***Melanie Swan, Founder, Institute for Blockchain Studies***

**Slides:** <http://slideshare.net/LaBlogga>

**Resources:** <https://github.com/ethereum/wiki/wiki>, <http://www.reddit.com/r/ethereum>

*We should think about the blockchain as another class of thing like the Internet – a comprehensive information technology with tiered technical levels and multiple classes of applications for any form of asset registry, inventory, and exchange, including every area of finance, economics, and money; hard assets (physical property); and intangible assets (votes, ideas, reputation, intention, health data, information, etc.)*

Current blockchain industry status:

- Bitcoin protocol ossifying, harder to make changes, network traction new alt.coins unlikely
- Solution1: Bitcoin overlay protocols (Mastercoin, Counterparty) ('http/smtp over TCP/IP')
- Solution 2: New foundational protocol (Ethereum) ('a new TCP/IP')
- Ethereum implements Satoshi's 3<sup>rd</sup> idea: (after (1) decentralized public ledger & (2) no third-party intermediary transactions)), (3) a scripting language for contracts (expand functionality from just currencies)

Ethereum: Bitcoin 2.0 protocol platform for smart contracts and decentralized applications

- Turing complete (can run any coin), blockchain + cryptographically-secure transactions
- Currency: Ether; \$18.4m raised 7/14; 40% p.a. money supply increase; Berlin dev space
- "Gas" fees charged on every computation to prevent attacks and abuse
- Ethereum virtual machine; a blockchain with a built-in programming language, a consensus-based globally executed VM; architecture: accounts, contracts, transactions

Concept: open-ended contracts to securely execute services including: voting systems, domain name registries, financial exchanges, crowdfunding platforms, company governance, self-enforcing contracts and agreements, intellectual property, smart property, and distributed autonomous organizations (DAOs)

1. Smart Contract: Transaction protocol that executes the terms of a contract
  - Smart property: property whose ownership is controlled via the blockchain using contracts (examples: cars, phones, houses); the blockchain becomes an inventory, tracking, and exchange mechanism for all hard assets
2. Dapp (Decentralized Application): contract plus graphical interface for contract execution (Javascript API 'eth object' interacts with Ethereum blockchain)
3. DAO (Decentralized Autonomous Organization): self-enforcing smart contract on a cryptographic blockchain
4. DAC (Decentralized Autonomous Corporations); automated markets; tradenets: fully-autonomous business entity, autonomous property, example: self-owned, self-driving car, example Storj.io (messages for daily data center storage quotes and self-relocates per price)

Progress areas: multi-sig, proof-of-stake, reputation systems, insurance, key recovery; Swarm (off-chain p2p data storage), Whisper (generalized messaging service (decentralized Twitter))