Blockchain
Part I

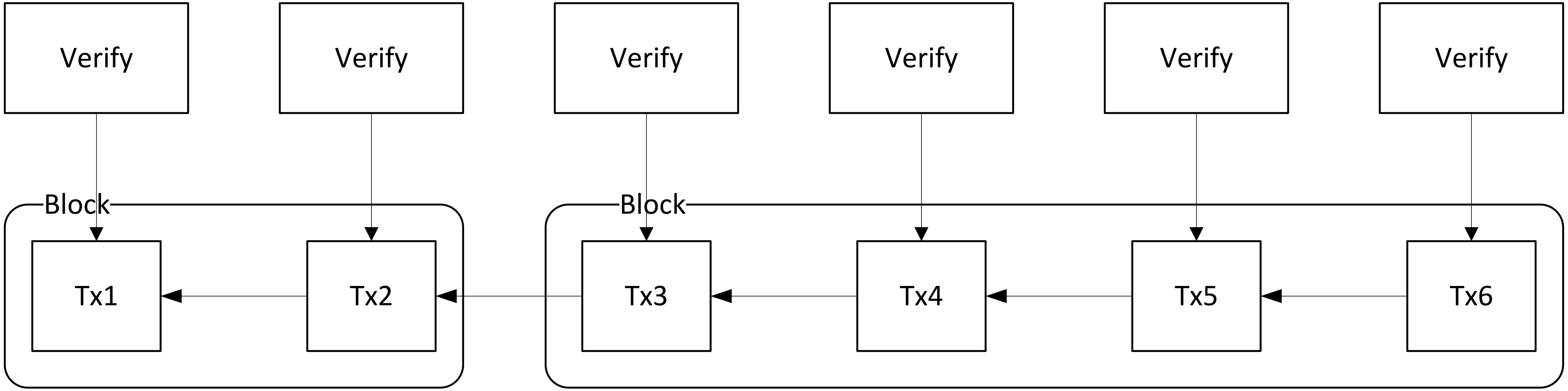
Garve.Hays@microfocus.com

MICRO® FOCUS

Presentation

- Introduce blockchain
- Discuss integration with identity management
- Part I: Background
- Part II: Demonstration and code (next time)

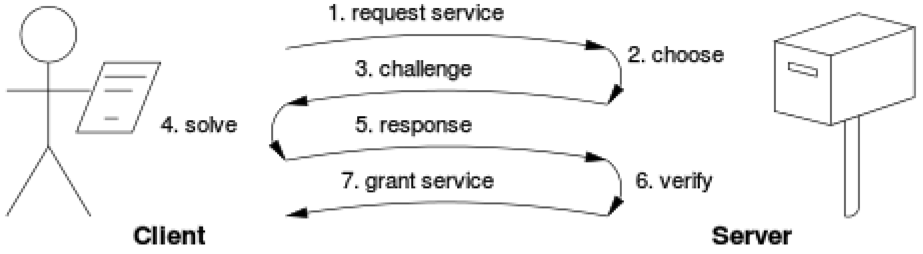
The Blockchain



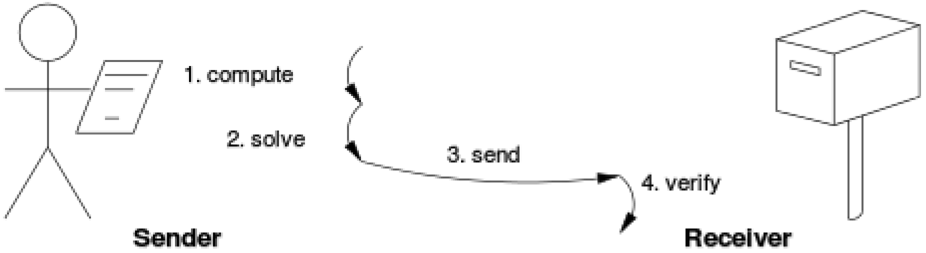
- Blockchain database == shared, public, distributed ledger
- Each block contains the hash of the previous one
- Each block holds a timestamp

Mining: Proof-of-Work

- Computationally expensive
- Used to “mine” bitcoins
- Generate hash and nonce
- Validate transactions



Challenge/Response



Solution/Verification

https://en.wikipedia.org/wiki/Proof-of-work_system

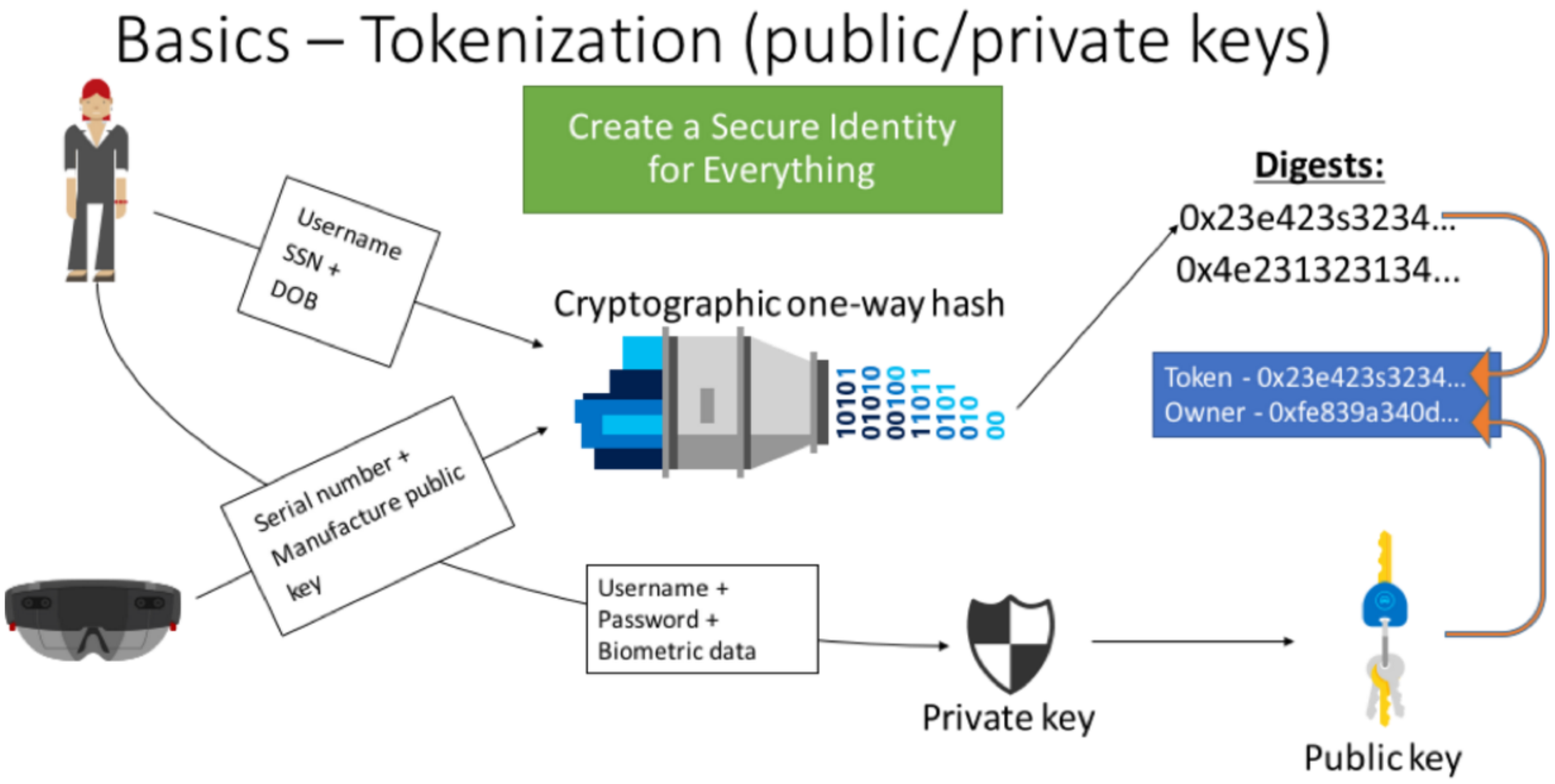
Proof-of-Stake

- Alternative to proof-of-work
- Distributed consensus algorithm
- Coin analogy: forged or minted vs. mined
- Less energy use (Mining == 240 kWh/bitcoin)

Tokens

- Cryptographically tokenized assets
- “Digital bearer bonds”
- Identity token
- Proof of identity (public/private) keys
- Digital token
  - Provenance
  - Ownership
  - Relationships
  - Lineage

Tokenization Process

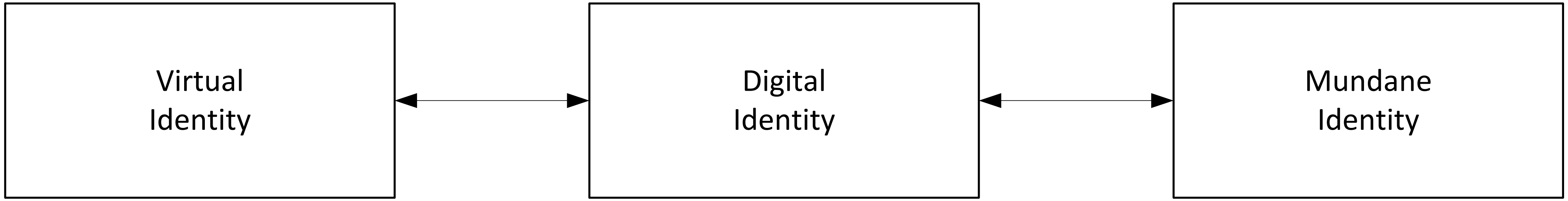

Basics – Tokenization (public/private keys)
Create a Secure Identity for Everything
Username SSN + DOB
Serial number + Manufacture public key
Cryptographic one-way hash
10101 01010 00100 11011 0101 010 00
Digests:
0x23e423s3234...
0x4e231323134...
Token - 0x23e423s3234...
Owner - 0xfe839a340d...
Username + Password + Biometric data
Private key
Public key

Source: https://github.com/Azure/azure-blockchain-projects/blob/master/bletchley/bletchley-whitepaper.md

Identity Management Integration

Identity Relationships

- Many-to-many relationships
- Digital Identity == Key Pair
- Mundane Identity == Real Life Person
- Virtual Identity == Public Key Certificate

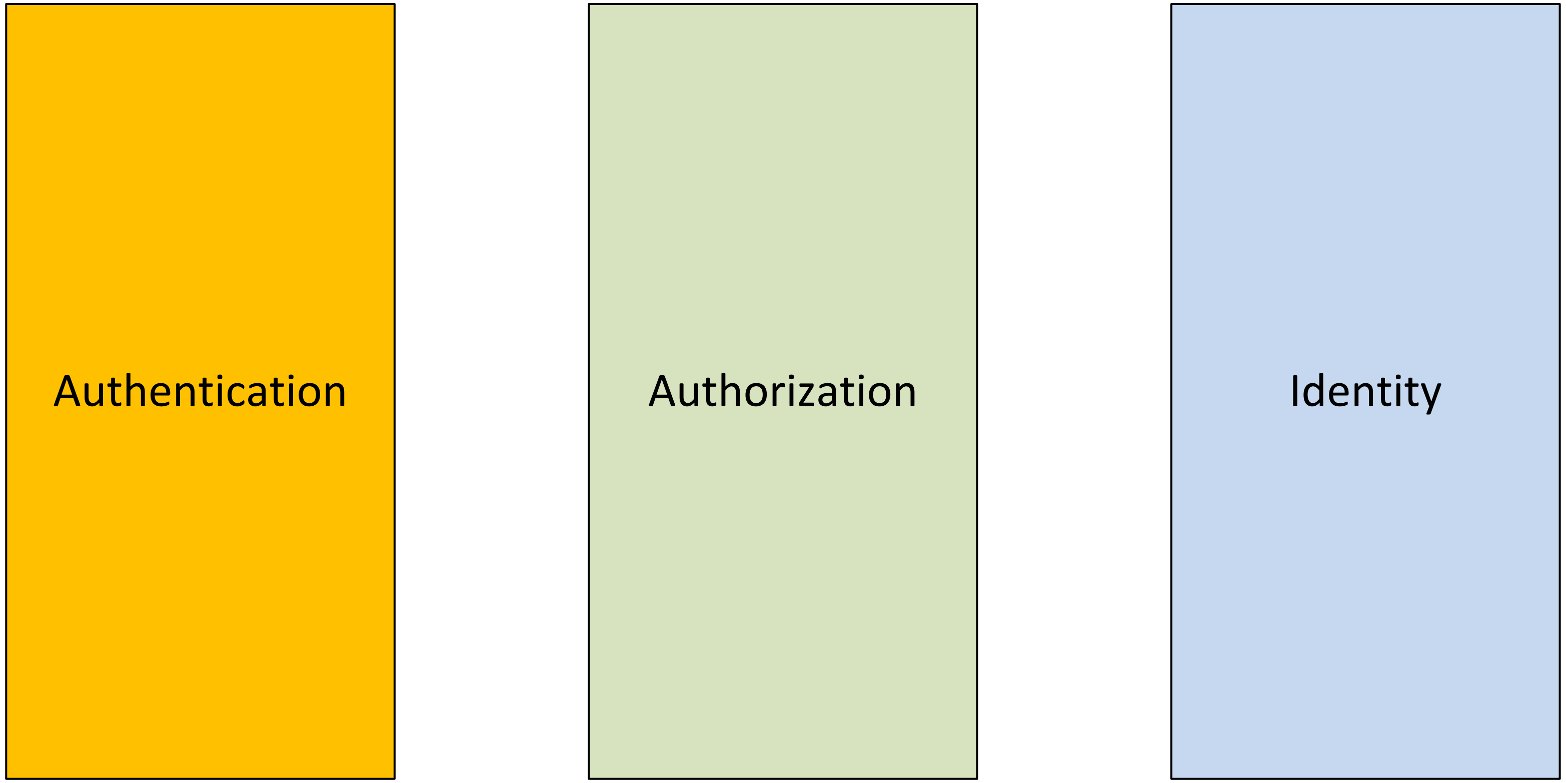


Identity Types

- Digital Identity == Key Pair
- Mundane Identity == Real Life Person
- Virtual Identity == Public Key Certificate

Use of Identities

- David Birch’s
- 3 domain model



Identification Domain

- Binding private key to mundane identity
- Passport
- Driver’s license
- Complicated and expensive
- When you are forced to reveal your real identity it opens you to identity theft

Authentication Domain

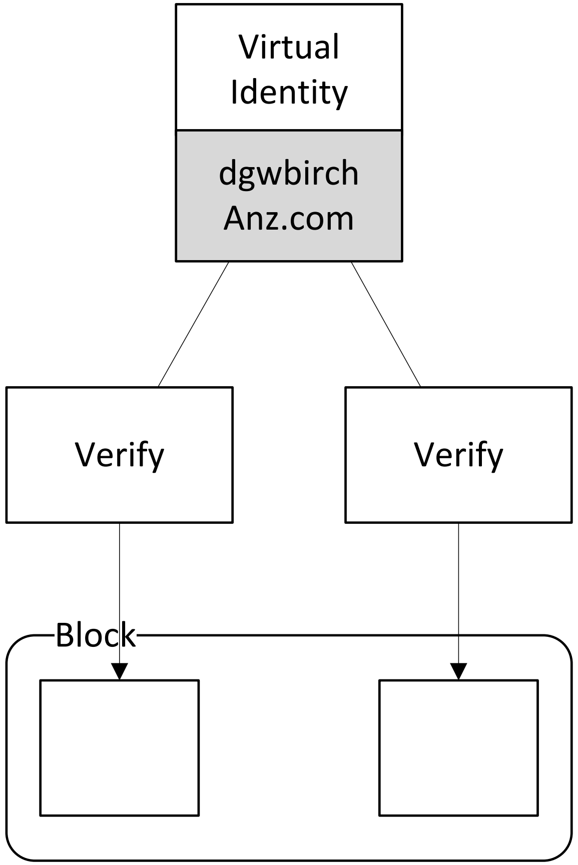
- Demonstrating you have control of the private key

Authorization Domain

- Where stuff gets done
- Interactions between virtual identities that are allowed to do stuff
- No more who are you questions
- What can you do?
- Are you allowed to access this bank account?
- Can you drive this car?
- Don’t ask who are you
- Don’t want to use your identity in transactions where ever possible

“Off Ledger”

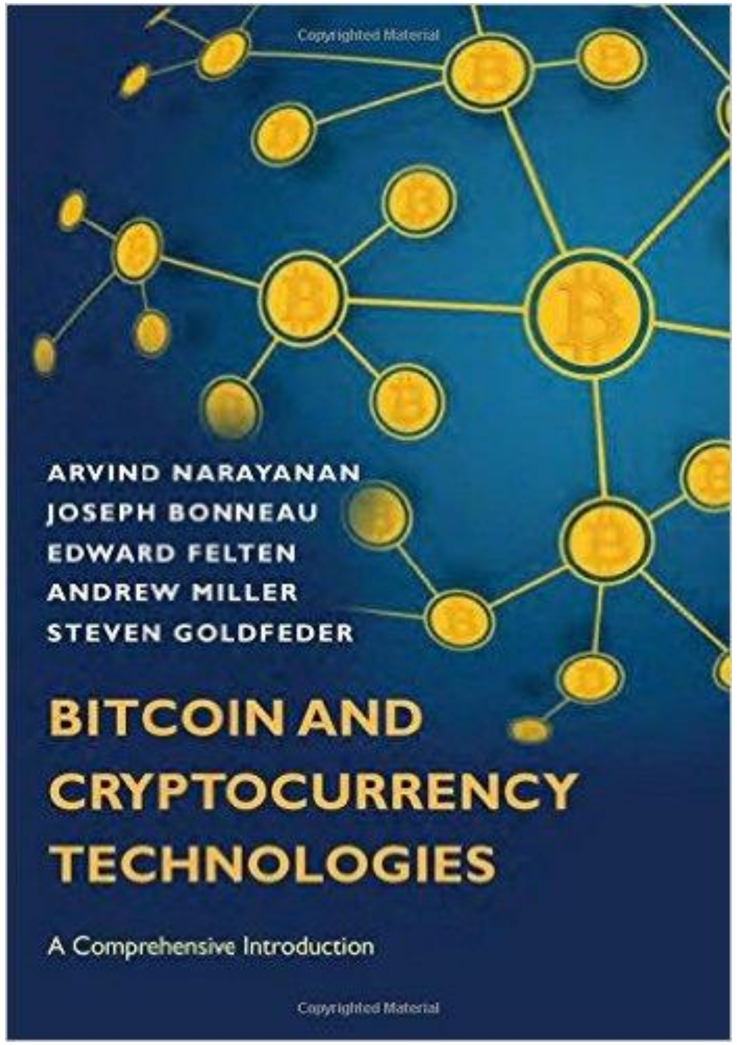
- Not stored on the blockchain
- A “smart contract” or distributed application is privy to this information



Ethereum

- Vitalik Buterin
- “Smart Contracts” or Distributed Applications
- Consensus Computer
- Distributed Nodes
- Ethash

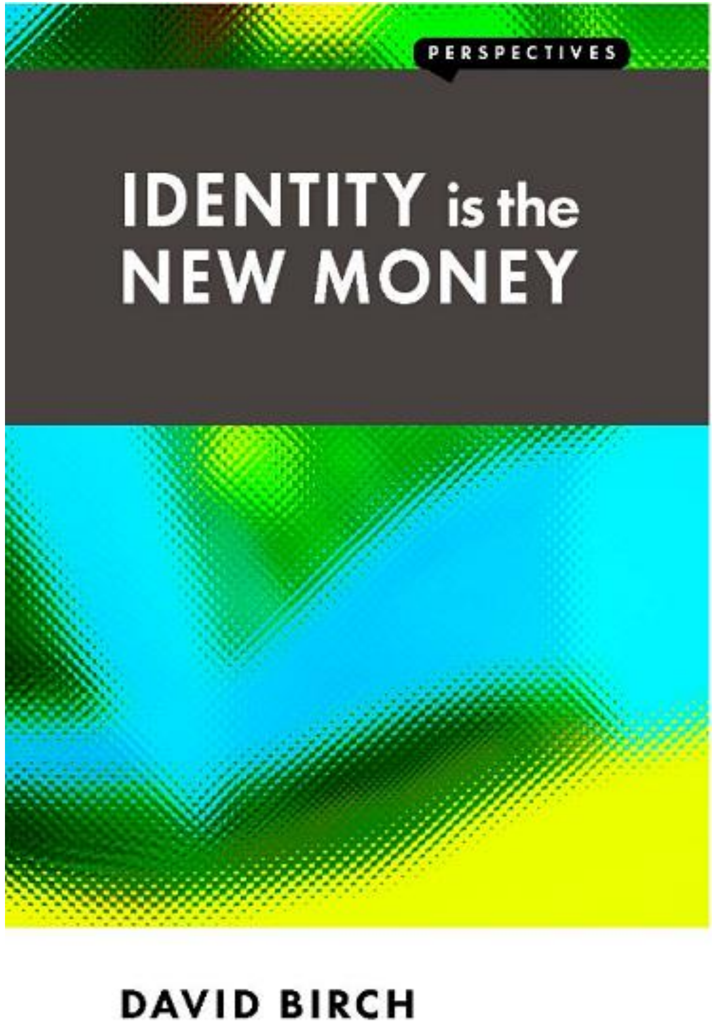
References



ARVIND NARAYANAN
JOSEPH BONNEAU
EDWARD FELTEN
ANDREW MILLER
STEVEN GOLDFEDER

BITCOIN AND CRYPTOCURRENCY TECHNOLOGIES

A Comprehensive Introduction



PERSPECTIVES

IDENTITY is the NEW MONEY

DAVID BIRCH

Links

- https://github.com/ethereum/go-ethereum/wiki/Command-Line-Options
- https://github.com/ethereum/go-ethereum/wiki/JavaScript-Console
- https://github.com/ethereum/go-ethereum/wiki/Building-Ethereum
- https://github.com/ethereum/wiki/wiki/Mining
- https://github.com/ethereum/wiki/wiki/Ethash (proof-of-work algorithm for Ethereum)
- https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ
- https://github.com/ethereum/pyethapp
- https://github.com/blockchain/api-v1-client-python
- https://github.com/blockchain/service-my-wallet-v3