Blockchain and Bitcoin – New Money

Sunil Sabat

Introduction Videos
https://www.youtube.com/watch?v=l9jOJk30eQs
https://www.youtube.com/watch?v=Lx9zgZCMqXE

Who Am I

- Sunil Sabat (MS Comp Eng., MS Comp Sc., and MBA)
- Certified - IBM, Microsoft, SNIA, Stanford Security and CompTIA.
- Co-authored IBM Redbook, published Big Data blogs at http://bidataknowhow.weebly.com, presented papers at various conferences (CompEuro, ISCAS,IBM Insight, Intel IPDT, GBDC and SV Code Camp)

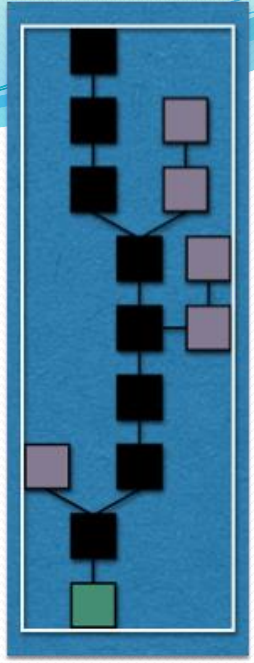
  - **Director of Product Management at Protegrity (Big Data Protection)**
  - **Owner of The Binayak Group (Education, Training and Enrichment)**
  - **Instructor at DataInquest**

  - **Worked at Intel as Chip IO Designer and CAD Engineer (first Pentium)**
  - **Worked at Cadence as Senior Consultant**
  - **Worked at IBM in Data Management Group (DB2, Infomix, Optim, Guardium)**
  - **Worked at Informatica as Principal Product Manager**
  - **Worked at startups that went IPO or were acquired**

Agenda

- Blockchain and Bitcoin Now
- Blockchain Fundamentals
- Blockchain Platforms (Ethereum, Chain.com,BigchainDB)
- Blcokchain Apps
  - Tokens , issue your own cryptocurrency
  - Ballots (Ethereum Cakeshop)
  - Commodities (Hyperledger)
- Labs
  - Crypto, Blockchain Simulator, Ethereum Cakeshop
  - Coinbase, Blockchain.info wallets
  - Mine as you read and more demos as time permits..

Blockchains: The Promise



HUFFPOST BUSINESS

Blockchain is a Disruption We Simply Have to Embrace

05/10/2016 01:34 pm ET | **Updated** 4 hours ago

By **SHANIKA GUNARATNA** / **CBSNEWS.COM** / *May 9, 2016, 7:22 AM*

Inside the tech that could "change the face of modern finance"

CBS money watch

NATO Innovation Contest Seeks Military Blockchain Applications

Stan Higgins | Published on May 10, 2016 at 17:21 BST

NEWS

CoinDesk

Schools are recording students' results using bitcoin tech

South China Morning Post EDITION:

INNOVATION

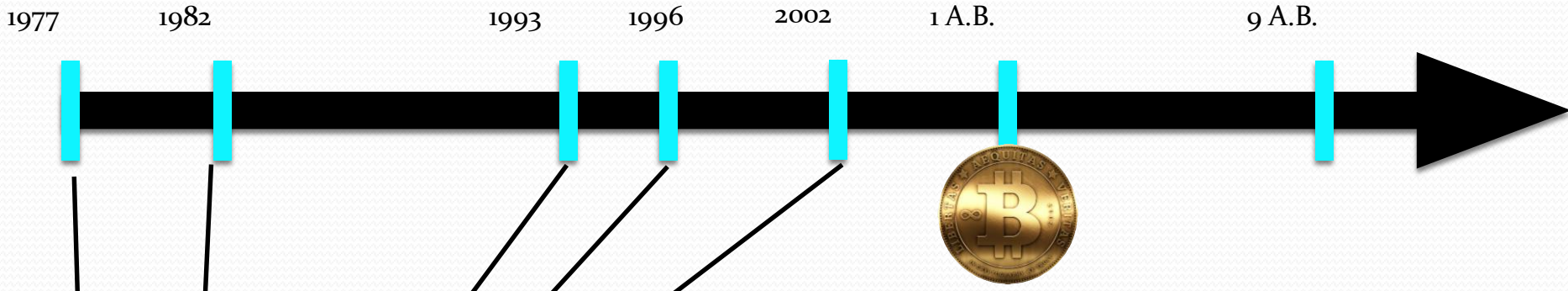
Real indices of promise

- Incredible array of participants here today:

- Bitcoin market cap: circa $7 Billion
- Blockchain VC funding to date: $1.1+ Billion
- Projected bank investment in 2017: $1 Billion[1]

[1]Source: Magister Advisors, http://magisteradvisors.com/blockchain-bitcoin-2016-a-survey-of-global-leaders/

31 B.B. Actually…



- RSA invented—digital currency an early proposed application
- Anonymous cryptocurrency introduced (Chaum)
- Proofs of work introduced (Dwork and Naor)
- First proof-of-work-based cryptocurrency (Rivest and Shamir)
- Karma: P2P currency

Bitcoin / blockchains underpinned by academic / scientific innovation

Overview: Early Money

- Early Intermediary Tokens of Exchange
  - Commodities or Objects of Perceived Worth
- Minted Coins → standardized units of metal
  - Code of Hammurabi: legal debt payment
- Trade Bills → credit certificate for production
  - Led to Local Merchant Banks for redemption
  - Goldsmiths → demand deposits & promissory notes

Introduction: What is Money?

- Physical or Electronic Tokens or Commodities that can be have the following properties:
  - **Unit of Account → defined value**
  - **Medium of Exchange → acceptability**
  - **Store of Value → non-perishable**

Beginnings of Modern Money

- Private Bank Notes
  - Loans based on deposits on account
  - Beginning of Fractional Banking

- National Currencies
  - from Central Reserve Banks
  - backed by Gold or Silver
  - Legal Tender for Payments

Modern Fiat Money

- **World War 1 & End of Gold Standard**
  - Scarcity of Gold Reserves with Enlarging Circulation
  - Bank Notes no longer redeemable for gold
  - Floating value in exchange market

- **Money by Decree of Government**
  - Backed by issuers ability to repay debts
  - Susceptible to public distrust
  - Possible uncontrolled inflation or deflation

What is Electronic Money?

- **Narrow View** of Term:
  - Tokens of Exchange transacted *only* electronically
  - Examples: Facebook Gold, Digital Gold Currency, BitCoin, and other electronic currencies
- **Broad Usage** of Term includes Both:
  - Electronic Payment Authorization → Credit cards
  - Value Holding Electronic Tokens
- A currency has value by it being widely used.

Types of Electronic Money

- **Private Currency** → free banking
- **Community Currency**→ local acceptability
- **World Currency** → trade reference
- **Hard Currency** → non-reversible
- **Soft Currency** → allows payment disputes

Private Currency

- **Free Banking → No Central Reserve Bank**
  - Free Entry into Banking Industry
  - Freedom to Issue Notes, Accept Deposits, and Collect Checks for Payment
  - Freedom to Borrow Money on Term Deposit
  - Freedom to Lend Money & Invest Assets

Community Currency

- **Ithaca HOURS**
  - Ithaca, NY
  - http://www.ithacahours.org/#whatareithacahours

- **BerkShares**
  - Berkshire, MS
  - http://www.berkshares.org/whatareberkshares.htm

- **Toronto Dollar**
  - Toronto, Ontario
  - http://torontodollar.com/aboutus/index.php

World Currency

- Global Trade Reference
  - Gold, British Pound, US Dollar, Euro, Yen
  - Private Complementary Currency efforts
- International Monetary Fund (IMF)
  - Special Drawing Rights (SDR)
  - Supplementary Reserve Assets

BitCoin

- It is simply a means of sending and receiving numbers to and from "addresses"
- An Open-Source Peer-To-Peer Payment Network
  - Using Digital Signatures & Encryption
    - decentralization is the basis for Bitcoin's security and freedom
- Public –Private Key Encryption
  - Alice & Bob Illustration
  - Digital Certificate Blocking Chain
- http://www.weusecoins.com/

Bitcoin

- **Governance** - an open source community of developers backed by the Bitcoin Foundation.
- **Democratic** - if you don't like one of the changes, you are more than welcome to fork the chain and implement your own rules
- **Money Creation** - is given to the people, not to the central bankers.
- **Deflationary** by design - money supply cannot be manipulated and is fixed at 21 million coins, each divisible up to 8 decimal

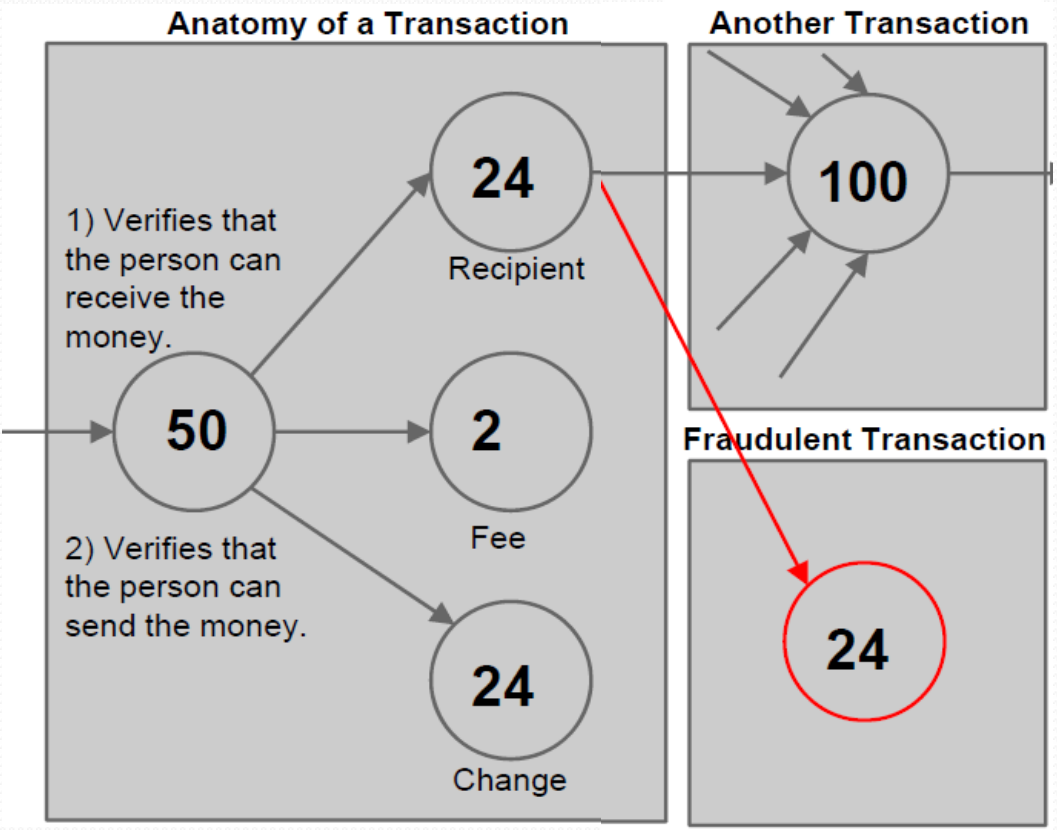
How it works

- The block chain is the fundamental data structure of the **Bitcoin protocol**.
- It's a single data file participants pass around to each other.
- It allows them to know who owns what.
- Anyone can change it to send money to someone else.
- Other users mathematically verify the transaction to ensure it's validity.

How It Works

- It's essentially an accounting ledger:
  1. 3/3/13 Sally found : $15.00
  2. 3/3/13 Sally -> Bob : $10.00
  3. 3/4/13 Bob -> Jimmy : $4.00
  4. 3/4/13 Sally -> Barb : $4.00
  5. 3/4/13 Jimmy -> Sally : $2.00
- How much money does Sally have in her wallet?
  - Sally had $15, then gave $10 to Bob, then $4 to Barb, then was given $2 from Jimmy. Sally has $3 as of right now.
  - Watch this - https://www.youtube.com/watch?v=l9jOJk30eQs

Transactions



Input contains

1) A public key that belongs to the redeemer of the output transaction.
2) An ECDSA hash over a hash of the transaction.

Output contains

1) The actual amount being sent to the recipient.
2) The change amount being sent back to the original sender (if any)
3) The voluntary transaction fee attached to the output (if any).

The **block chain** prevents the double spend attack by giving other nodes the power to verify that transaction inputs were not already spent somewhere else.

Block Chain

- Bitcoin makes sure there is only one block chain by making blocks really hard to produce.
- Miners have to compute a **cryptographic hash** of the block that meets certain criteria
  - difficulty of the criteria for the hash is adjusted based on how frequently blocks are appearing
  - **also carefully validate all the transactions that go into their blocks**
- Successful miners are rewarded some bitcoins according to a preset schedule

Mining

- Miners collect the transactions on the network into large bundles called **blocks**
  - like "Alice pays Sam 10 bitcoins" and “David pays Sofia 8.3 bitcoins".
- These blocks are strung together into one continuous, authoritative record called the **block chain**,
  - which doesn't permit any conflicting transactions.
  - *lets you know for sure exactly which transactions count and can be trusted* (no double spending!).
  - Trusted and Collaborative

BitCoin Mining

1. Collects transactions from the network
2. Validates them, and doesn't allow conflicting ones
3. Puts them into large bundles called blocks
4. Computes cryptographic hashes over and over until if finds one "good enough to count"
5. Then submits the block to the network, adding it to the block chain and earning a reward in return
6. Miners mine bitcoin rewards for mining a block
   - **The block reward is halved every 210,000 blocks, or roughly every 4 years. The block reward started at 50 in 2009, is now 25 in 2014, and will continue to decrease.**

Reference :

1. https://en.bitcoin.it/wiki/Mining
2. https://99bitcoins.com/bitcoin-mining-profitable-beginners-explanation/
3. http://www.investopedia.com/terms/b/bitcoin-mining.asp

Let us mine now

- Lab
  - Go to https://qz.com/154877/by-reading-this-page-you-are-mining-bitcoins/
  - Read article and mine
  - See output and ask any questions.

Fraud prevention

- Users can trust the block chain that was most difficult to produce
  - longest chain wins
- If there was a "fake" blockchain competing with the real ones the fraudster would have to do as much work as the rest of the network to make their block chain look as trustworthy
  - Intense work that goes into finding blocks through hashing secures the network against fraud
  - Read https://qz.com/154877/by-reading-this-page-you-are-mining-bitcoins/

Bitcoin Security

- Bitcoin addresses are *RACE Integrity Primitives Evaluation Message Digest* RIPEMD-160 of *SHA-256* of an *Elliptic Curve Digital Signature Algorithm* public key
  - any vulnerabilities in the algorithms would constitute a vulnerability in bitcoin itself
- An attacker with > 50% of hash power can
  - *Double spend*: Reverse transactions that he sends while he's in control
  - Prevent some or all transactions from gaining any confirmations
  - Prevent some or all other generators from getting any generations

Roadmap's Overarching Goals

2015-2017:	Send, receive, find, and use priority data domains to improve health care quality and outcomes.
2018-2020:	Expand data sources and users in the interoperable health IT ecosystem to improve health and lower cost.
2021-2024:	Achieve nationwide interoperability to enable a learning health system, with the person at the center of a system that can continuously improve care, public health, and science through real-time data access.

Blockchain and Cloud

Azure Blockchain solutions

Ethereum Consortium

Microsoft

STRATO Blockchain LTS

BlockApps

Chain Core Developer Edition

Chain

Ethereum Studio - Blockchain

ether.camp

Emercoin Blockchain

Emercoin

More – IBM and AWS

Fully managed Blockchain-as-a-Service

IBM Blockchain on Bluemix Beta

Fully managed blockchain-as-a-service on the most secure operating environment

Self-managed

IBM signed and certified Docker image of Hyperledger Fabric

A free solution to package and release software that can be run on any environment that supports docker images

IBM premium blockchain support

A technical support service by IBM experts deeply involved in the Hyperledger Fabric project

AWS does not believe in choosing **one** protocol to rule them all…

- Building an ecosystem that can be tapped into by different use cases and industries is our main focus
- Enabling experimentation into maturity
- Leveraging our services to enact a robust solution

Technologies to look into:

AWS CloudTrail
AWS CloudFormation
AWS WAF
Amazon ECS
Amazon EBS volume

Kubernetes
Amazon S3
Auto Scaling
Amazon VPC/Route 53
AWS IAM

Google Cloud

If the tests are successful, cloud services could potentially play a role in blockchain deployments, since a database shared by multiple companies is more easily managed in the cloud. Worldwide, the public cloud services market should reach $204 billion this year, up from $175 billion last year, according to researcher Gartner Inc.

- Banks to use Google data centers for tests of new technology
- Royal Bank of Scotland tries out a clearing and settlement app

Google's cloud services will be used to test blockchain technologies for banks, an area where IBM, Microsoft and Amazon have been courting clients for the past year.

Royal Bank of Scotland Group has employed Google servers in a trial of a new blockchain application for clearing and settlement, the consulting firm GFT said Friday in a statement. The company's cloud services will also be used by other bank clients of the firm, Stuttgart, Germany-based GFT said.

Until now, International Business Machines Corp. and Microsoft Corp. have been most active in rolling out special developer tools and inviting banks and start-ups to test the new database technology in their massive data centers. Amazon.com Inc., the leader in cloud service, has also been working with blockchain startups. GFT is a member of Google Cloud Platform's Partner Program.

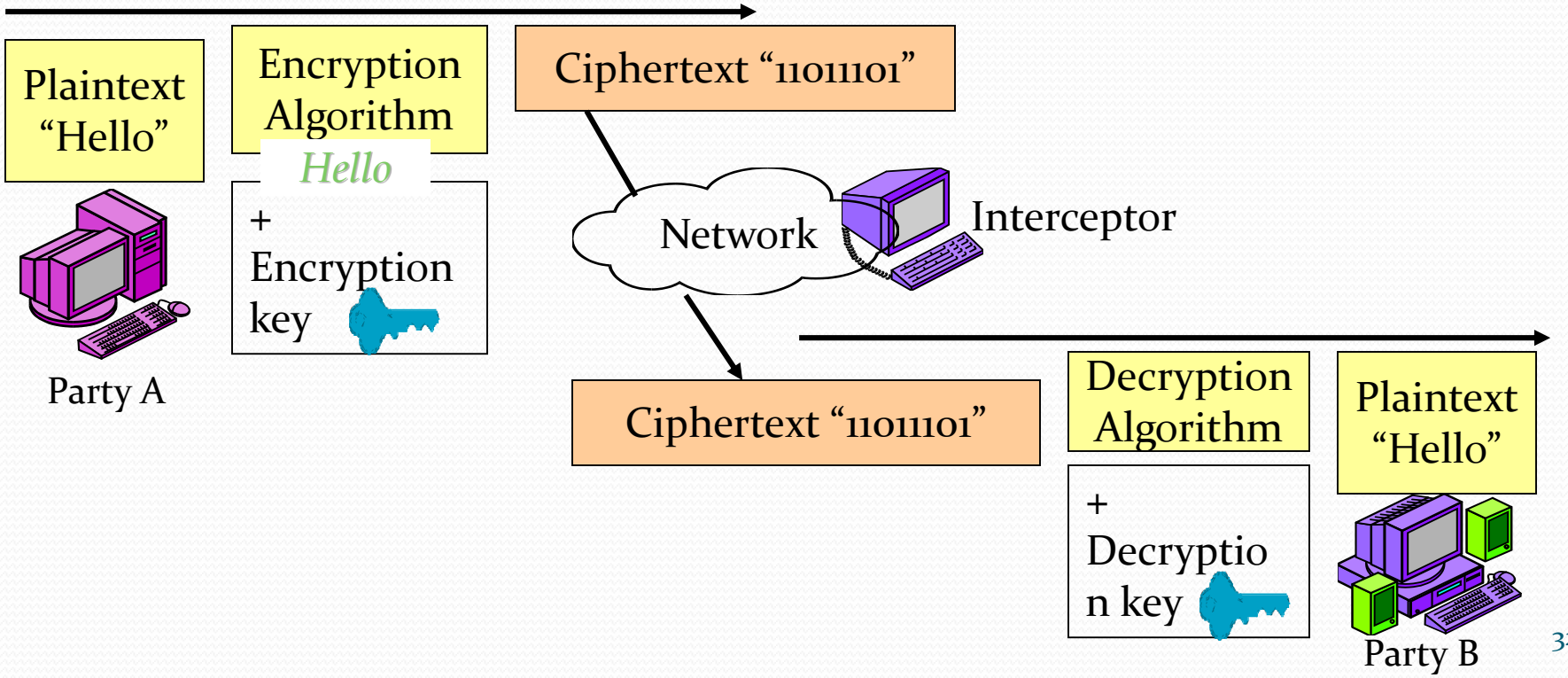
The blockchain is a distributed ledger where multiple companies -- such as banks -- can record transactions securely. The database's strength lies in its trustworthiness: the difficulty of reversing or changing any transactions that have been recorded. By facilitating trust and collaboration, the technology promises to make many industries more efficient, and reduce costs on everything from international money transfers to paying a supplier.

Cryptography?

- Traditionally, *cryptography* refers to
  - The practice and the study of encryption
  - Transforming information in order to prevent unauthorized people to read it.
- Today, *cryptography* goes beyond encryption/decryption to include
  - Techniques for making sure that encrypted messages are not modified en route
  - Techniques for secure identification/authentication of communication partners.

Basic Terminology 1

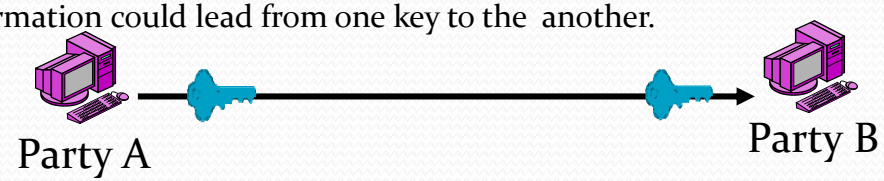
- **Plaintext:** original message to be sent. Could be text, audio, image, etc.
- **Encryption/Decryption Algorithm:** mathematical tool (software) used to encrypt or decrypt
- **Key:** A string of **bits** used by to encrypt the plaintext or decrypt the ciphertext
- **Ciphertext:** encrypted message. Looks like a random stream of bits



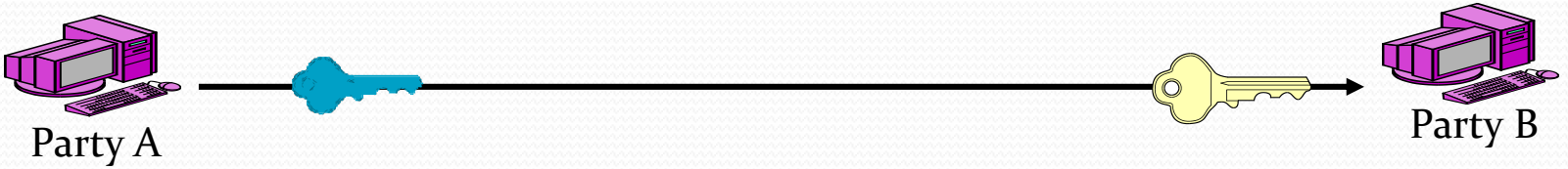
Basic Terminology 2

- Encryption:
  - Converting plaintext into ciphertext using algorithms and keys
  - The size of the ciphertext is proportional to the size of the plaintext
  - Ciphertext is reversible to plaintext
- Symmetric Key Encryption:
  - Same key is used both for encryption and decryption
  - Keys are usually identical or trivially identical*

* Trivially identical means simple transformation could lead from one key to the another.



- Asymmetric Key Encryption:
  - Also called Public/Private Key Encryption
  - Two different keys are used: one for encryption, one for decryption



Online Encrypt: | https://www.tools4noobs.com/online_tools/

Exhaustive search and Key length

- Attacker could use the right algorithm and do an exhaustive search (i.e. try all possible keys) in order to decrypt the ciphertext
- Most attacks require the capture of large amount of ciphertext
- Every additional bit in the length of the key doubles the search time
- Every additional bit in the length of the key doubles the requirements in terms of minimum processor's speed to crack the key.

Key Length in bits	Number of possible keys ($2^{\text{key length in bits}}$)
1	2
2	4
4	16
8	256
16	65536
56	72057594037927900
112	5192296858534830000000000000000000 or 5.1923E+33
168	3.74144E+50
256	1.15792E+77
512	1.3408E+154

Weak vs. Strong Keys

- Symmetric Key Encryption
  - Usually for private of customer e-business
  - Keys < 100-bit long are considered weak today.
  - Keys **100-bit long or more** are considered strong today.
- Asymmetric Key Encryption
  - Usually used for B2B e-commerce
  - Key pairs must be much longer (512 bit and more) because of the disastrous consequences of breaking the decryption key

Key Length in bits	Number of possible keys ($2^{\text{key length in bits}}$)	Type of communication
1	$2^1 = 2$	
2	$2^2 = 4$	
16	$2^{16} = 65536$	
56	$2^{56} = 72057594037927900$	Private, symmetric, weak asymmetric (e.g. DES)
100	$2^{100} =$	Private, symmetric
112	$2^{112} = 5192296858534830000000000000000000$ or 5.1923E+33	Business, asymmetric (e.g. 112-bit DES)
168	3.74144E+50	Business, asymmetric (e.g. 3DES)
256	1.15792E+77	Business, asymmetric (e.g. AES)
512	1.3408E+154	Business, asymmetric (e.g. RSA)
1024 to 4096	2^{1024} to 2^{4096}	Business, asymmetric (e.g. RSA)

Symmetric Key Encryption

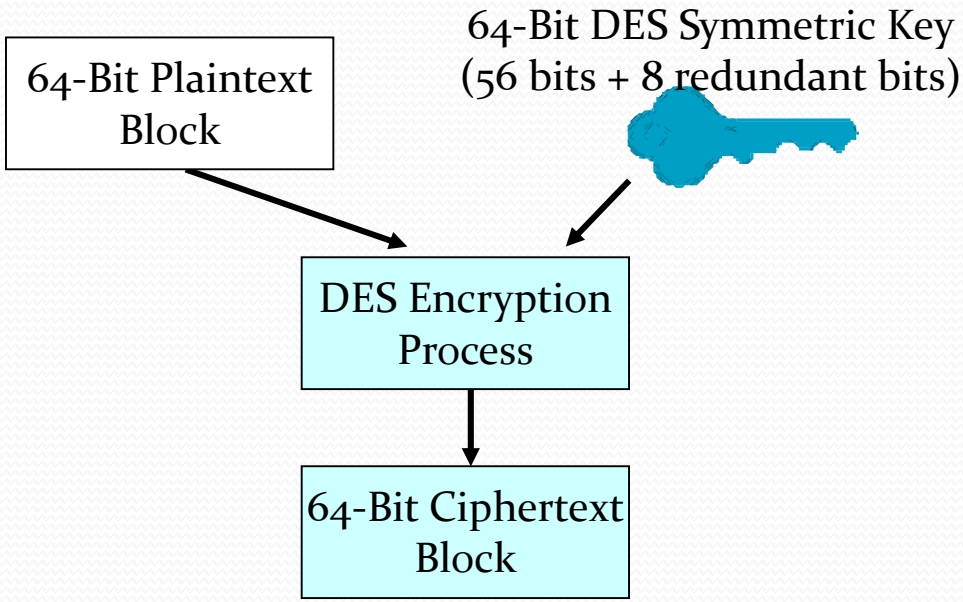
Symmetric Key Encryption methods

- Two categories of methods
  - Stream cipher: algorithm operates on individual bits (or bytes); one at a time
  - Block cipher: operates on fixed-length groups of bits called *blocks*
- Only a few symmetric methods are used today

Methods	**Year approved**	**Comments**
Data Encryption Standard - DES	1977	1998: Electronic Frontier Foundation's Deep Crack breaks a DES key in 56 hours
DES-Cipher Block Chaining		
Triple DES – TDES or 3DES	1999	
Advanced Encryption Standard – AES	2001	Its versions among the most used today
Other symmetric encryption methods		
IDEA (International Data Encryption Algorithm), RC5 (Rivest Cipher 5), CAST (Carlisle Adams Stafford Tavares), Blowfish		

Data Encryption Standard (DES)

- DES is a block encryption method, i.e. uses block cipher
- DES uses a 64 bit key; actually 56 bits + 8 bits computable from the other 56 bits
- Problem: same input plaintext gives same output ciphertext



DES, 3DES, and AES

	DES	3DES	AES
Key Length (bits)	56	112 or 168	128, 192, 256
Key Strength	Weak	Strong	Strong
Processing Requirements	Moderate	High	Modest
RAM Requirements	Moderate	High	Modest

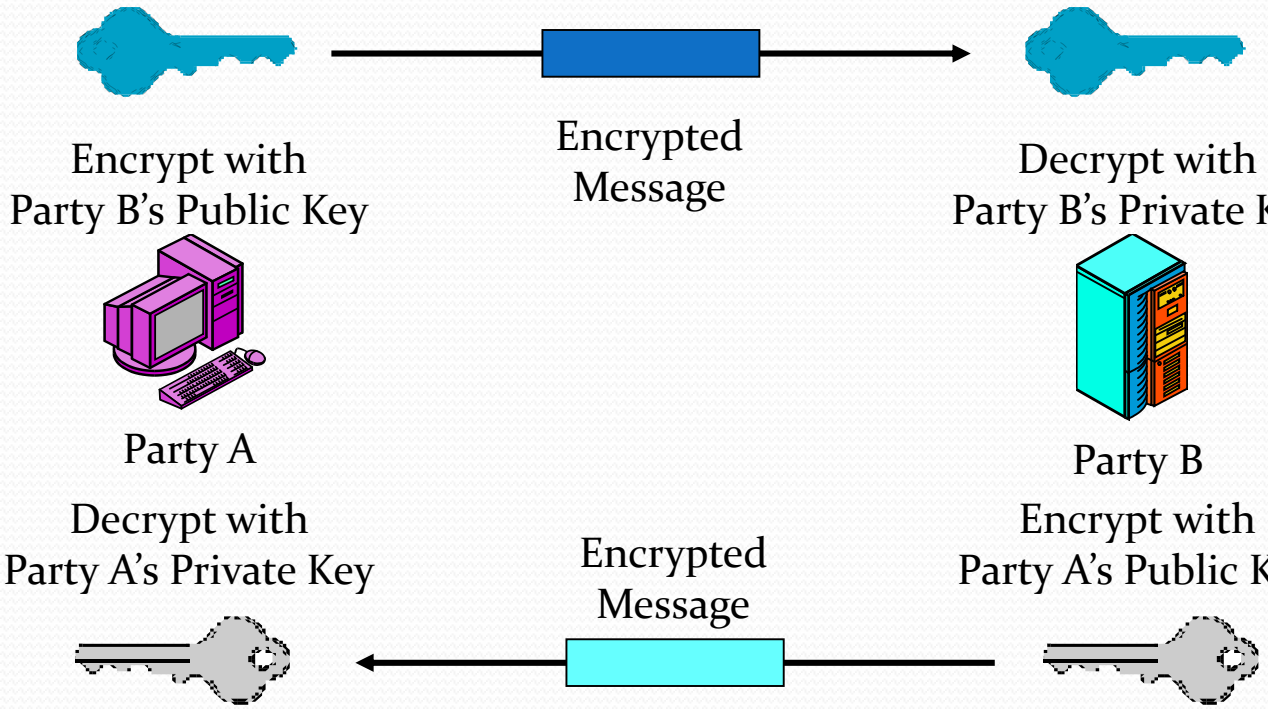
Encryption Algorithms Used by MS Operating Systems

Operating System	Default Algorithm	Other Algorithms
Windows 2000	DESX	(none)
Windows XP RTM	DESX	3DES
Windows XP SP1	AES	3DES, DESX
Windows Server 2003	AES	3DES, DESX
Windows Vista	AES	3DES, DESX
Windows Server 2008	AES	3DES, DESX (?)

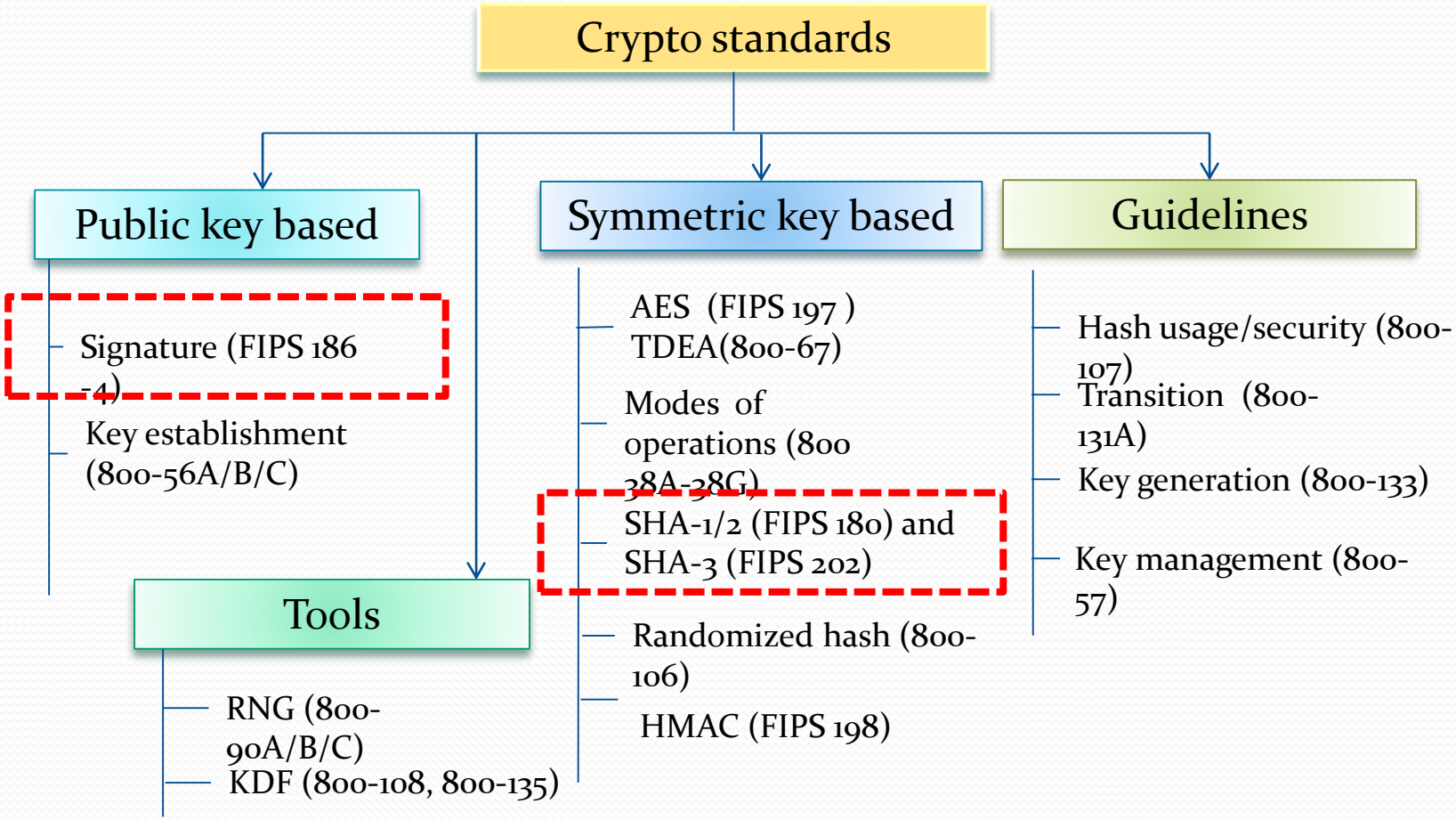
Asymmetric Key Encryption

Public Key Encryption For confidentiality

- Each Party uses other party's public key for encryption
- Each Party uses own private key for decryption
- No need to exchange private key, but key needs to be very strong (512+ bit)



NIST Crypto Standards - Overview



Development procedures for new cryptographic standards

- Cryptographic algorithm competitions
  - Advanced Encryption Standard (AES)
  - Secure Hash Algorithm – 3 (SHA-3)
- Adoption of standards developed in other standards organizations (e.g. SP 800-56A, SP 800-56B)
- Develop new standards
  - In-house development based on well accepted research results (e.g. SP 800-56C)
  - Selected among submissions (e.g. modes of operations in 38 series)

Blockchain Books

Shop for apress blockchain book on Google

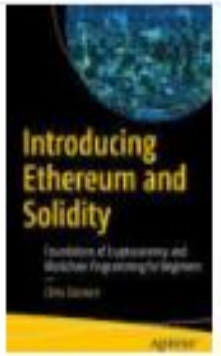
Sponsored

Blockchain Basics (ebook)
$13.22
Google Play

Blockchain Basics - Drescher
$14.99
Apress.com
Free shipping

The Blockchain Alternative - ...
$19.99
Apress.com
Free shipping

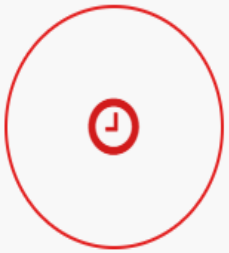
Blockchain Basics: A Non-...
$18.98
Barnes & Noble



Introducing Ethereum and ...
$35.55
Barnes & Noble
Free shipping

ARK

ARK provides users, developers, and startups with innovative blockchain technologies. Accessible via push button clone-able blockchains, and our SmartBridge technology. ARK aims to create an entire ecosystem of linked chains and a virtual spiderweb of endless use-cases that make ARK highly flexible, adaptable, and scalable. ARK is a secure platform designed for mass adoption and will deliver the services that consumers want and developers need.



FAST

ARK's Core is configured to produce ultra fast transactions with 8 second blocktimes. With easily implemented future scaling, higher throughput is available whenever ARK needs it.

DECENTRALIZED

ARK provides a more decentralized voting system than other DPoS consensus models. Voting weight is divided across all votes instead of assigning 100% weight to each vote, making it nearly impossible for a takeover of

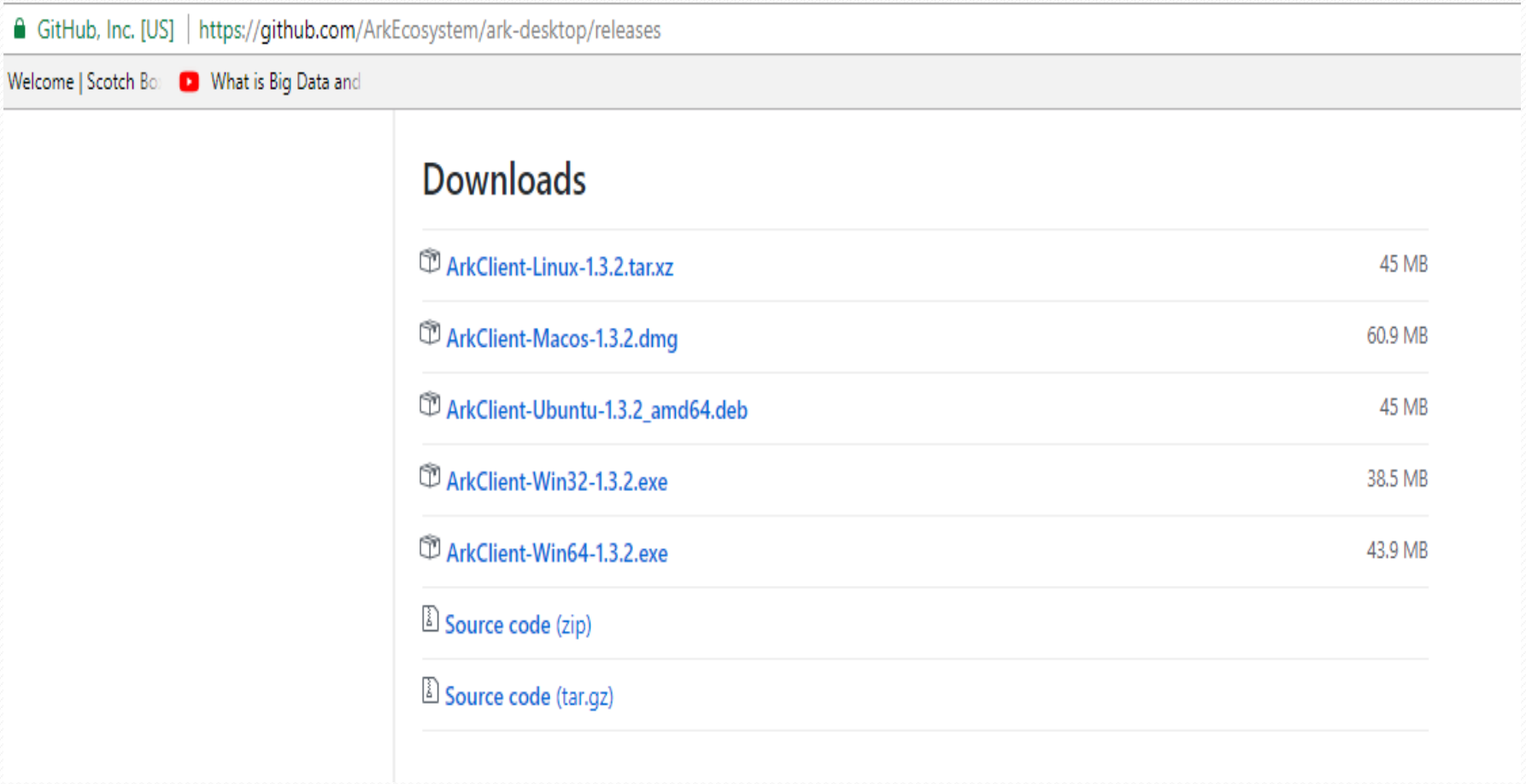
BRIDGING

ARK aims to bridge well known blockchain technologies through the use of SmartBridges, making an interconnected ecosystem of blockchains possible.

SUSTAINABLE

The ARKShield program provides an extra layer of protection to ARK. A professionally managed Sustainability and Contingency Fund or ARKShield, will provide stable funding throughout future development.

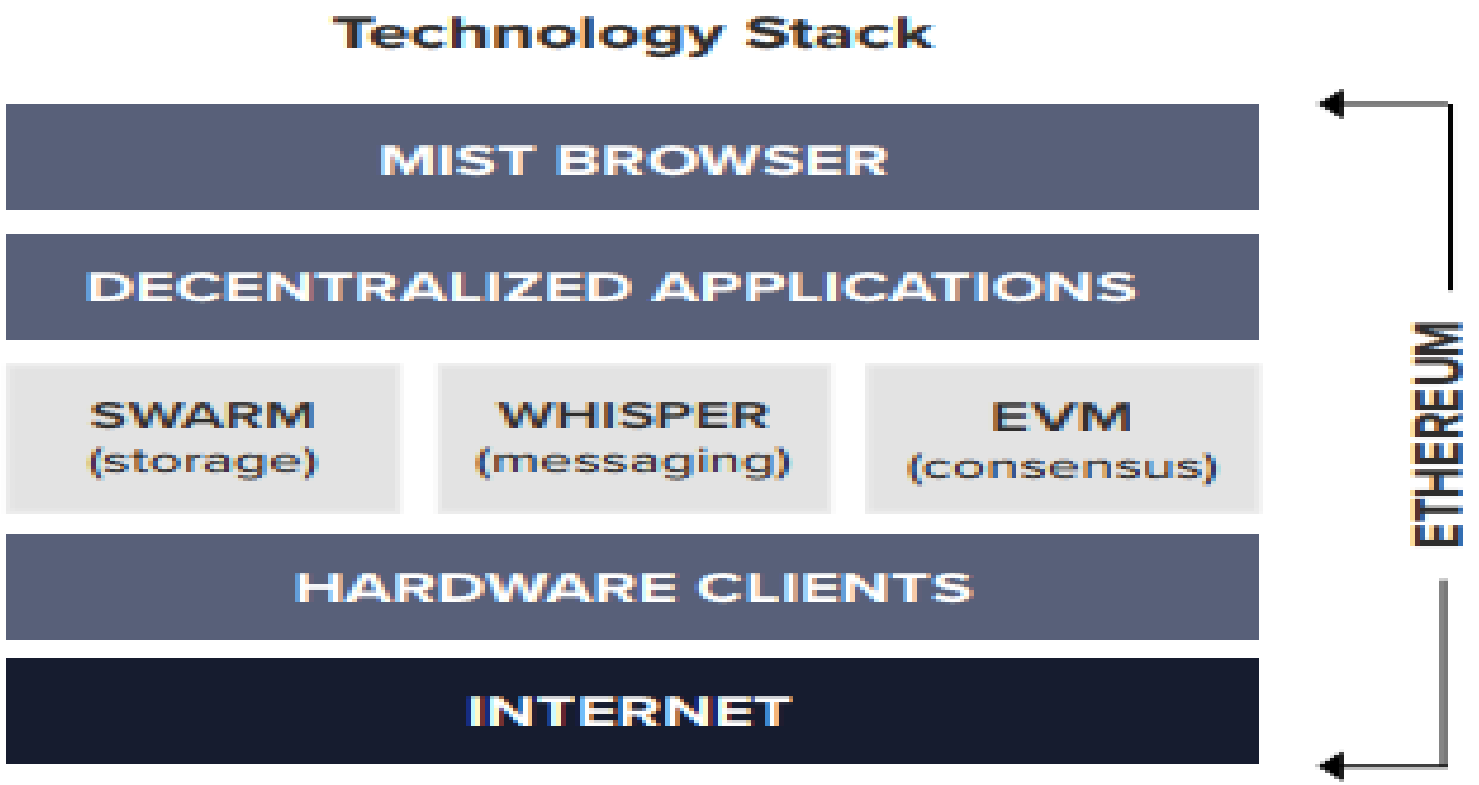
ARK Client


GitHub, Inc. [US] | https://github.com/ArkEcosystem/ark-desktop/releases
Welcome | Scotch Bo
What is Big Data and
Downloads
ArkClient-Linux-1.3.2.tar.xz
45 MB
ArkClient-Macos-1.3.2.dmg
60.9 MB
ArkClient-Ubuntu-1.3.2_amd64.deb
45 MB
ArkClient-Win32-1.3.2.exe
38.5 MB
ArkClient-Win64-1.3.2.exe
43.9 MB
Source code (zip)
Source code (tar.gz)

Ethereum Background

- Consists of a non-exhaustive list of components includes a cryptographic token and address system, a network of miners, a consensus algorithm, a blockchain ledger, the ethereum Virtual Machine, a set of programming languages and complex economic structures.
- **Applications**
  - A platform that would enable thousands of digital currencies to operate on the same network, with the goal being an “economic democracy” that would enable more efficient funding of philanthropic and other difficult-to-finance societal goods.
  - Decentralized autonomous organizations. New forms of digital entities could be built to manage shared resources under a set of terms and conditions enshrined in code and empowered by the collective decisions of stakeholders.
  - Smart contracts. New contracts could be built that instead of being enforceable through a legal system, would programmatically enforce themselves.
  - Smart property. The definition of property would expand with the idea that cryptographic, blockchain-based tokens could serve as representations of real world assets, like museum passes or tickets.

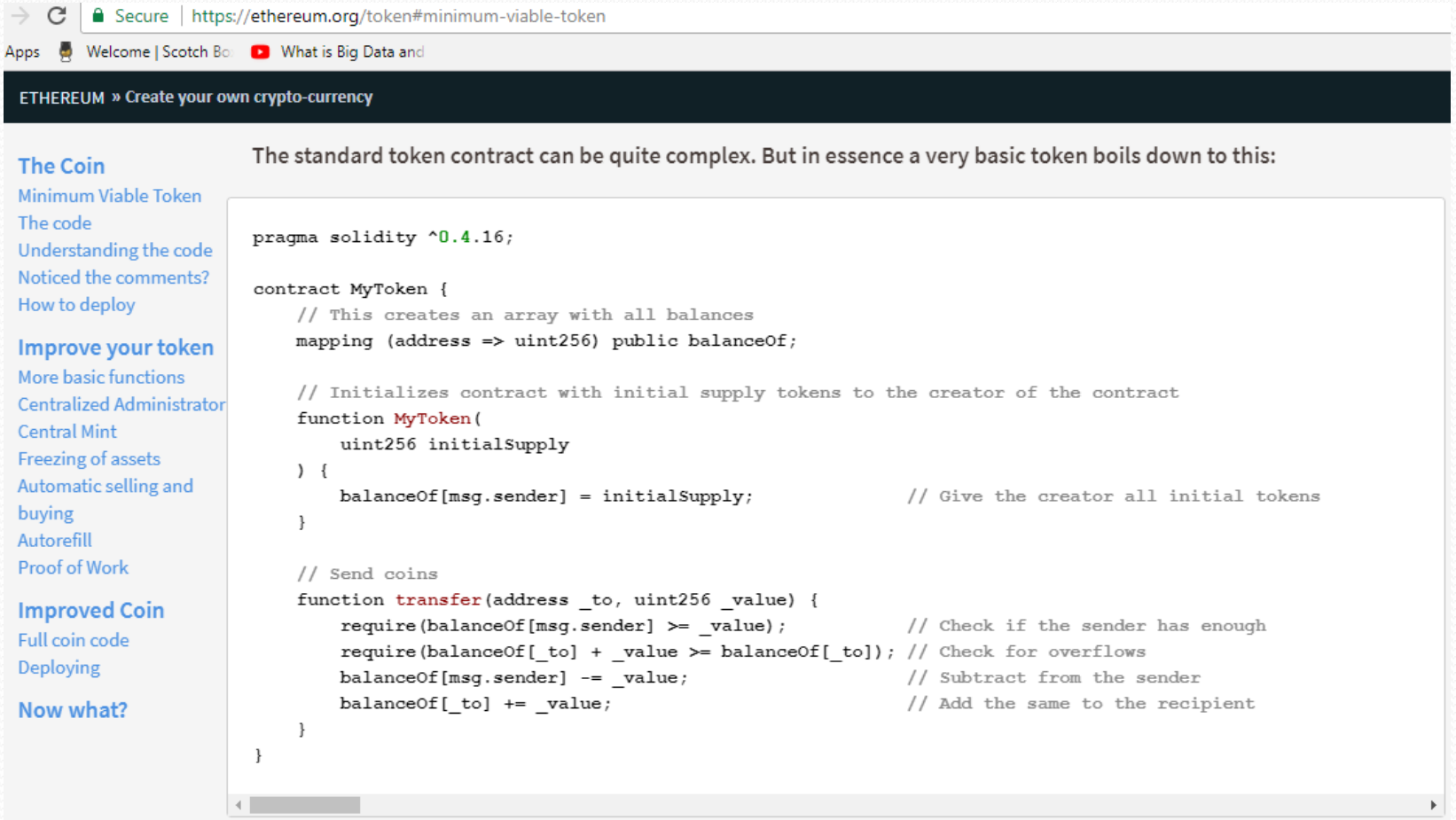
Architecture



Solidity Language

- Solidity lets you program on Ethereum, a blockchain-based virtual machine that allows the creation and execution of smart contracts, without requiring centralized or trusted parties.
- Solidity is a statically typed, contract programming language that has similarities to Javascript and C. Like objects in OOP, each contract contains state variables, functions, and common data types.
- Contract-specific features include modifier (guard) clauses, event notifiers for listeners, and custom global variables.
- Some Ethereum contract examples include crowdfunding, voting, and blind auctions.
- Review code at https://learnxinyminutes.com/docs/solidity/

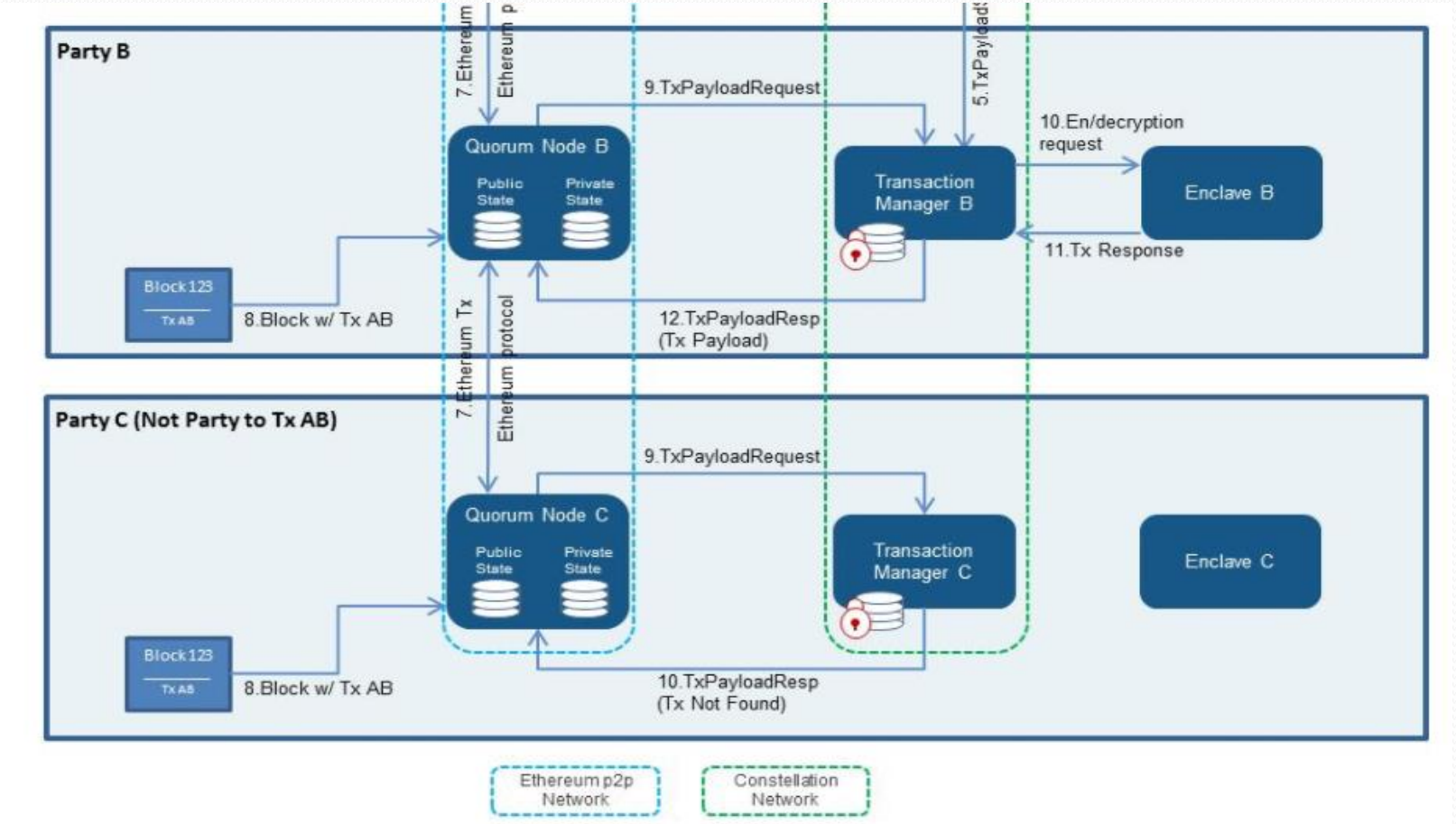
Simple Token



JPMC – Quorum - Cakeshop

- Quorum is an Ethereum-based distributed ledger protocol with transaction/contract privacy and new consensus mechanisms.
- Quorum is a fork of go-ethereum and is updated in line with go-ethereum releases.
- Key enhancements over go-ethereum:
  - **Privacy** - Quorum supports private transactions and private contracts through public/private state separation and utilising Constellation, a peer-to-peer encrypted message exchange for directed transfer of private data to network participants
  - **Alternative Consensus Mechanisms** - with no need for POW/POS in a permissioned network, Quorum instead offers multiple consensus mechanisms that are more appropriate for consortium chains:
    - **QuorumChain** - a new smart-contract based, majority voting consensus model
    - **Raft-based Consensus** - a consensus model for faster blocktimes, transaction finality, and on-demand block creation
  - **Peer Permissioning** - node/peer permissioning using smart contracts, ensuring only known parties can join the network
  - **Higher Performance** - Quorum offers significantly higher performance than public geth

Quorum Architecture



JPMC - Cakeshop

- An integrated development environment and SDK for Ethereum-like ledgers
- *Cakeshop* is a set of tools and APIs for working with Ethereum-like ledgers, packaged as a Java web application archive (WAR) that gets you up and running in under 60 seconds.
- Included in the package is the geth, quorum, and constellation Ethereum servers, a Solidity compiler and all dependencies.
- It provides tools for managing a local blockchain node, setting up clusters, exploring the state of the chain, and working with contracts.

BigchainDB

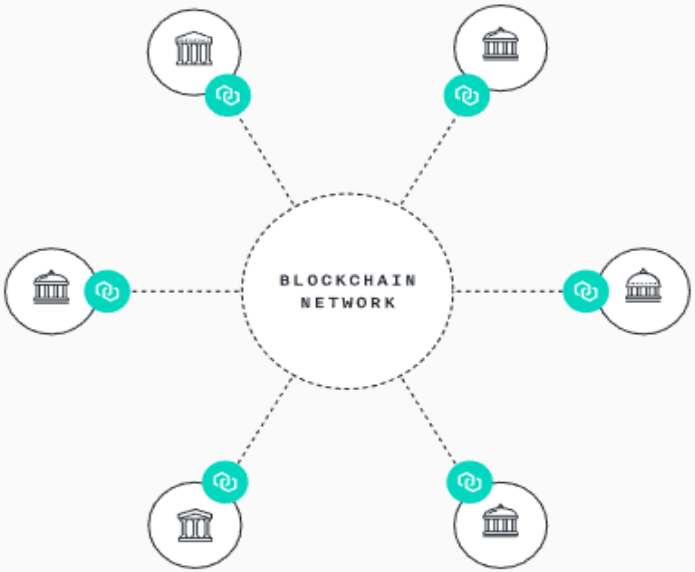
- BigchainDB is a scalable blockchain database. That is, it's a "big data" database with some blockchain characteristics added, including decentralization, immutability and native support for assets.
- At a high level, one can communicate with a BigchainDB cluster (set of nodes) using the BigchainDB Client-Server HTTP API, or a wrapper for that API, such as the BigchainDB Python Driver.
- Each BigchainDB node runs BigchainDB Server and various other software. The terminology page explains some of those terms in more detail.

Big Data and Block Chain

We built BigchainDB on top of an enterprise-grade distributed DB, from which BigchainDB inherits high throughput, high capacity, a full-featured NoSQL query language, efficient querying and permissioning.

	Bitcoin Blockchain	Distributed Database	BIGCHAIN DB
Immutability	✓		✓
No Central Authority	✓		✓
Assets Over Network	✓		✓
High Throughput		✓	✓
Low Latency		✓	✓
High Capacity		✓	✓
Rich Permissioning		✓	✓

CITI – Chain.com



Using **Chain Core,** institutions can launch and operate a blockchain network, or connect to a growing list of other networks that are transforming how assets move around the world.

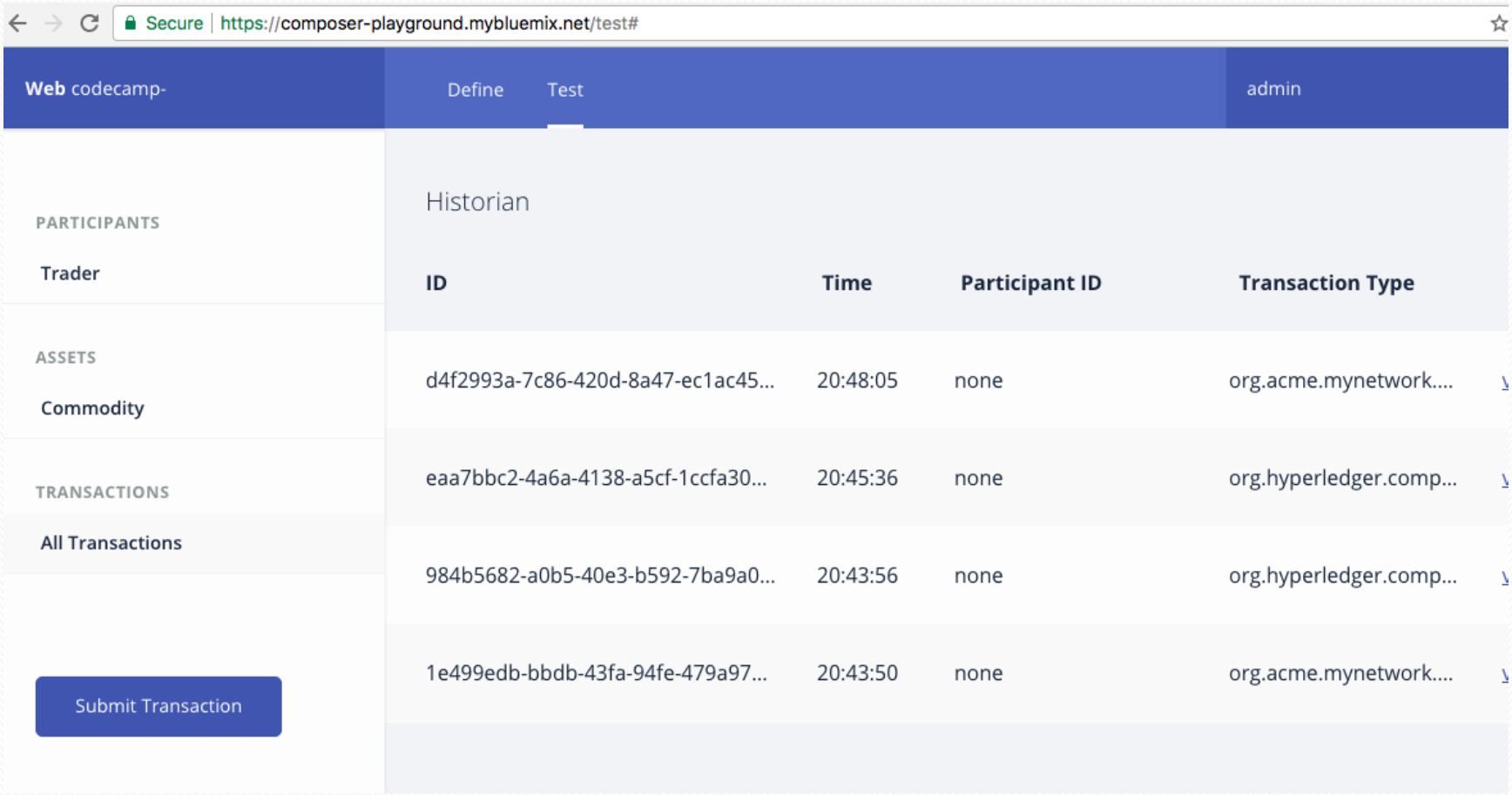
CITI – Chain.com

- Chain Core is software designed to operate and participate in permissioned blockchain networks. Each network maintains a cryptographically-secured multi-asset shared ledger. Using this ledger, participants can issue digital assets directly to custodians, who can then transfer them to each other in real time with no transactional intermediary.
- Each Chain Core holds a copy of the ledger and independently validates each update. A federation of block signers ensures global consistency of the ledger.
- Digital assets share a common, interoperable format and can represent any units of value that are guaranteed by a trusted issuer — such as currencies, bonds, securities, IOUs, or loyalty points.

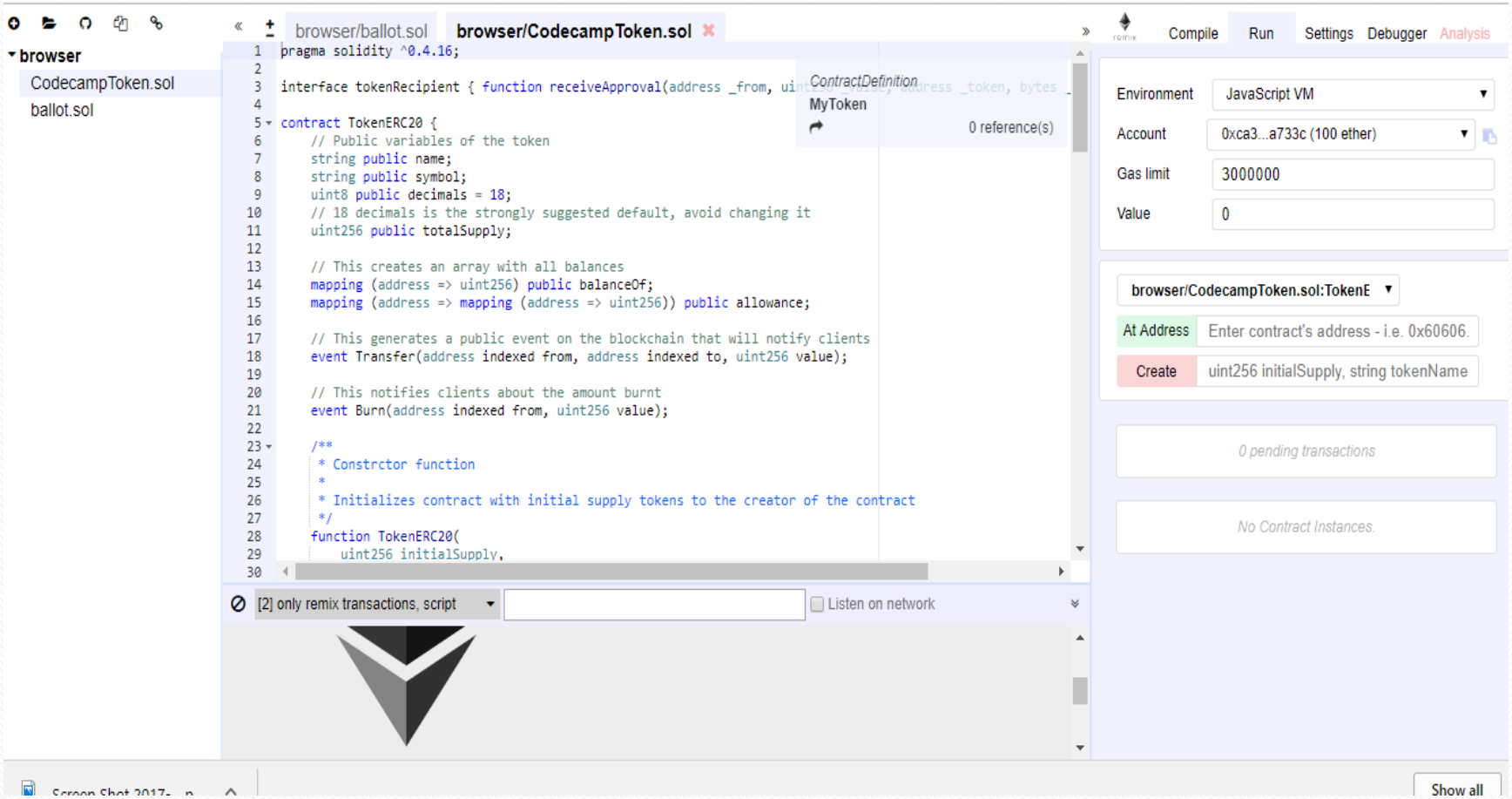
ICO

- **So, what is an ICO?**
- An Initial Coin Offering (ICO) enables funding of projects through the sale of tokens or cryptocoins, which are similar to shares of a company, ***though usually without equity being exchanged.***
- Investors and supporters of the project can purchase them through an Initial Public Offering (IPO) transaction with fiat (say, USD or Euro) or cryptocurrencies (like Ethereum). An ICO usually sets a minimum goal for the fundraise and a period of time to reach that goal—not unlike a Kickstarter.

Hyperledger Transactions



Remix browser solidity code



End

Thank You.