Blockchain Technology

Salil Donde

Salil Donde

ventiv TECHNOLOGY

Nasdaq

LEWTAN™ Acquired by Moody's Analytics

MSB Marshall & Swift/Boeckh Acquired by TPG

AlphaPoint

fiserv.

Let's talk about….

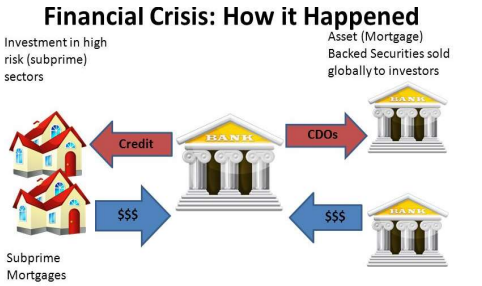
The Rise of Blockchain

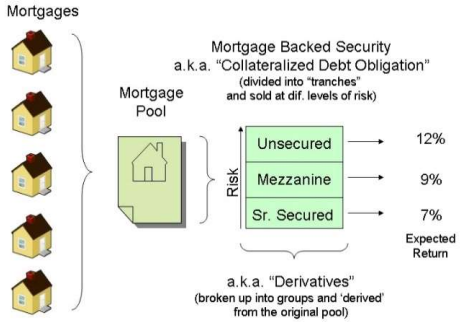
- Financial Crisis of 2007-08
- Bitcoin – How it started

Blockchain Technology Today

- Bitcoin – The inner working
- The Underlying Principles
- The Technology / Platform
- Blockchain Benefits

Financial Crisis of 2008 - 09





https://www.youtube.com/watch?v=ACbV9PchvNo
https://www.youtube.com/watch?v=5y85Ss9pFQk

What Happened?

5 key attributes of illiquid assets:

1. Lack of price discovery
2. Lack of transparency,
3. An element of counter-party risk,
4. No guarantee of settlement
5. High frictional costs.

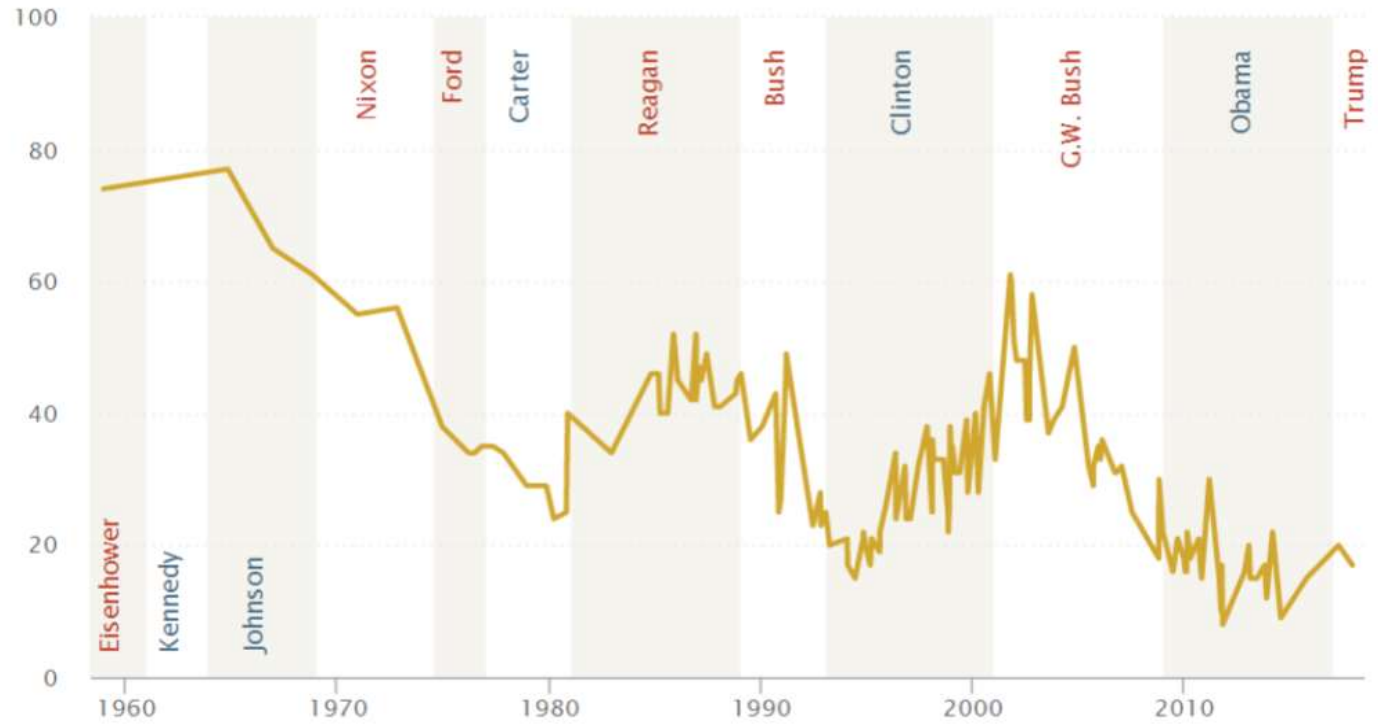
Alive and well in a very important and large asset class: Asset Backed Securities and Mortgage Backed Securities.

The hidden fraud and the lack of transparency caused the value in this asset class to crumble, thereby bringing down the entire financial system, globally for several years.

Trust In Government

Trust in U.S. government at 60-year lows...

Figure: Trust in U.S. Government at 60-year lows
% who trust the US government in Washington always or most of the time



Bitcoin, cryptocurrency : Blockchain the enabler

92 Percent of Millennials ***Don't Trust Banks***

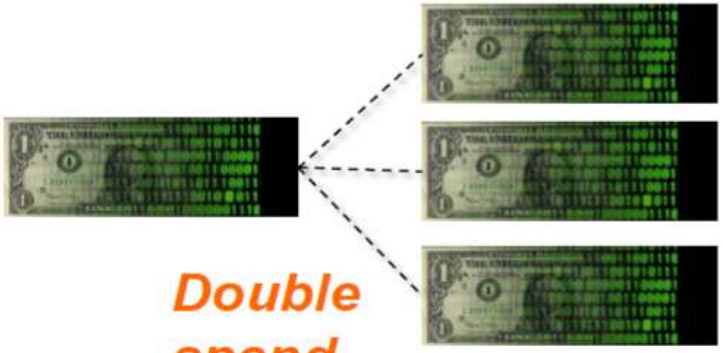
Earlier in 2016, Facebook IQ, a team of researchers, scientists and analysts funded and supported by Facebook Inc., published a white paper entitled "**Millennials + money: The unfiltered journey**" to evaluate the beliefs and thoughts of today's youth on traditional banking and financial systems. **The paper found that 92 percent of millennials firmly expressed their distrust of banks.**

Blockchain enables digital money to exist with Trust

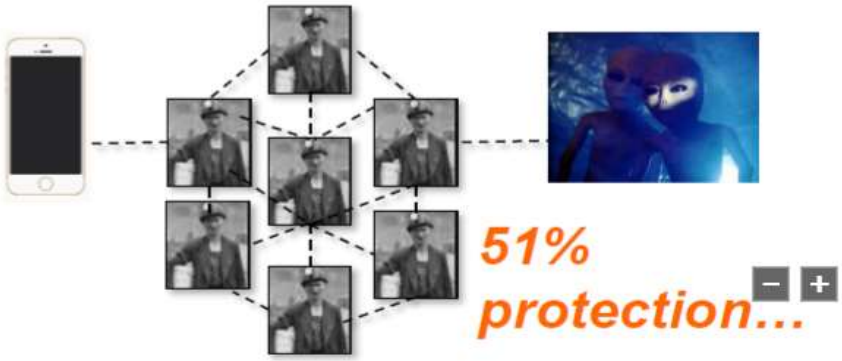
Paper money

Credit card / Electronic

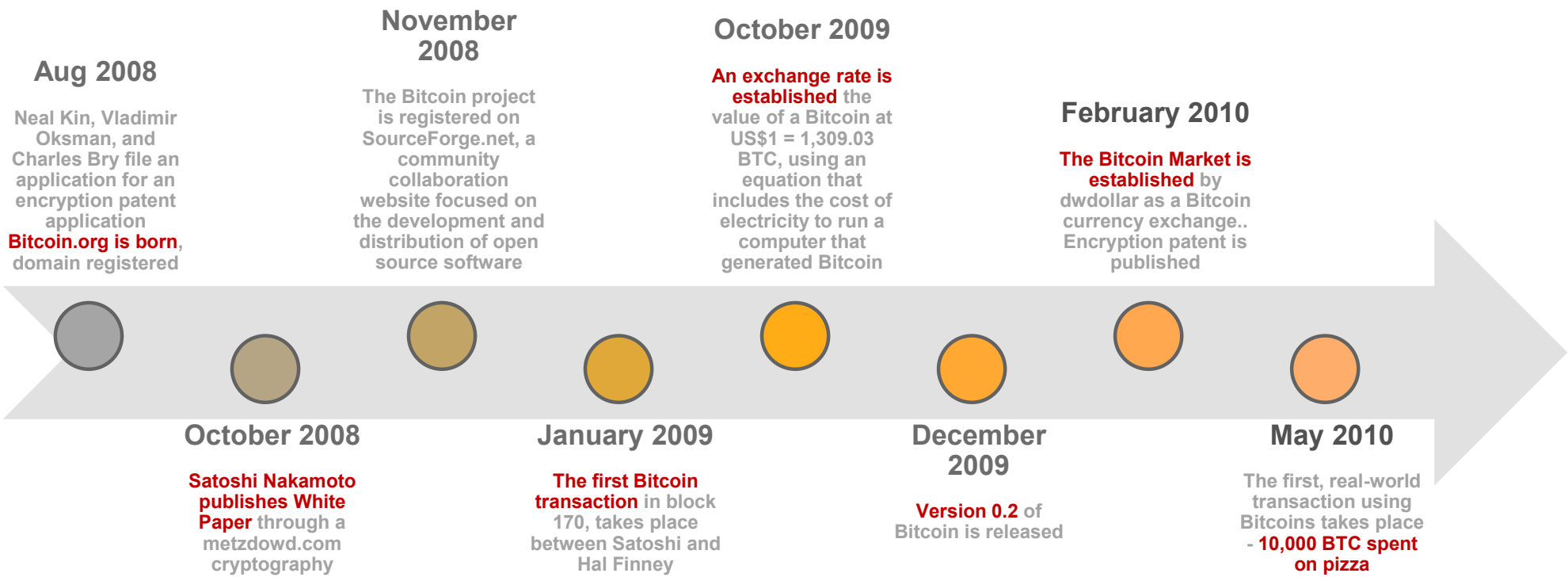
Digital money



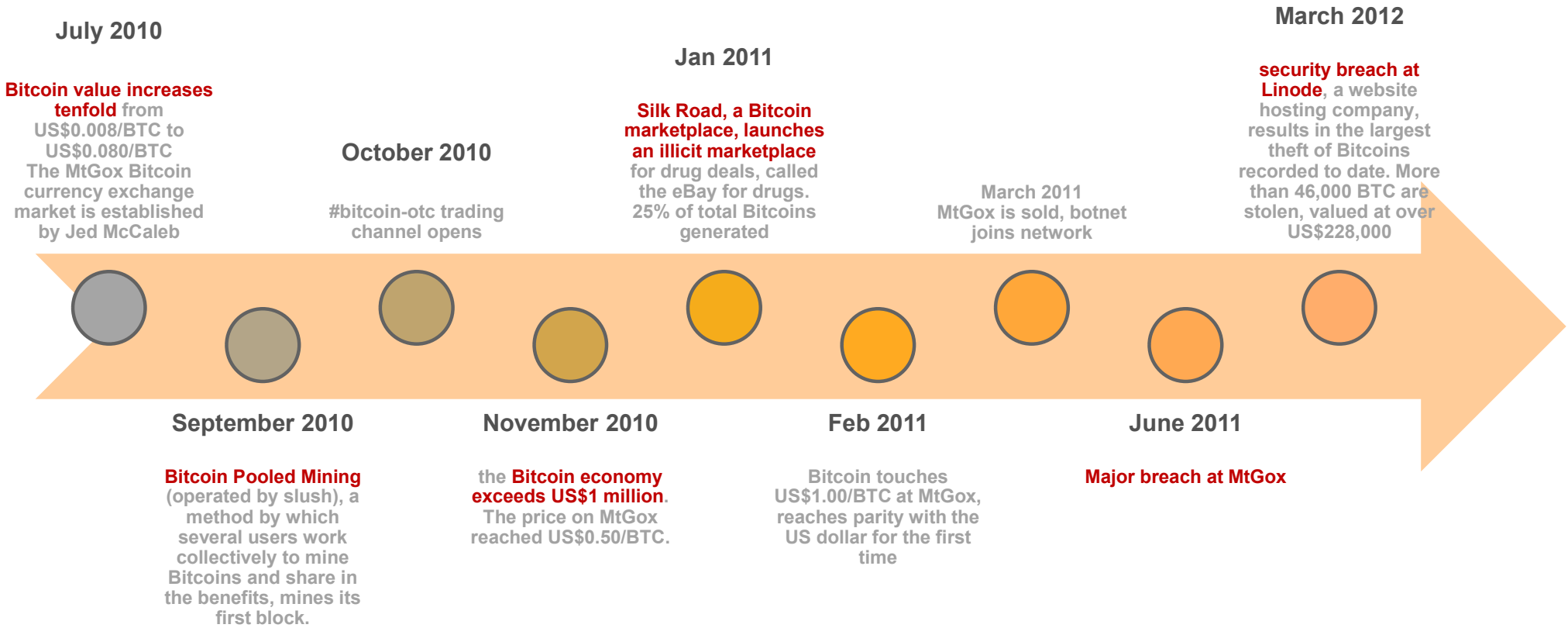
Blockchain



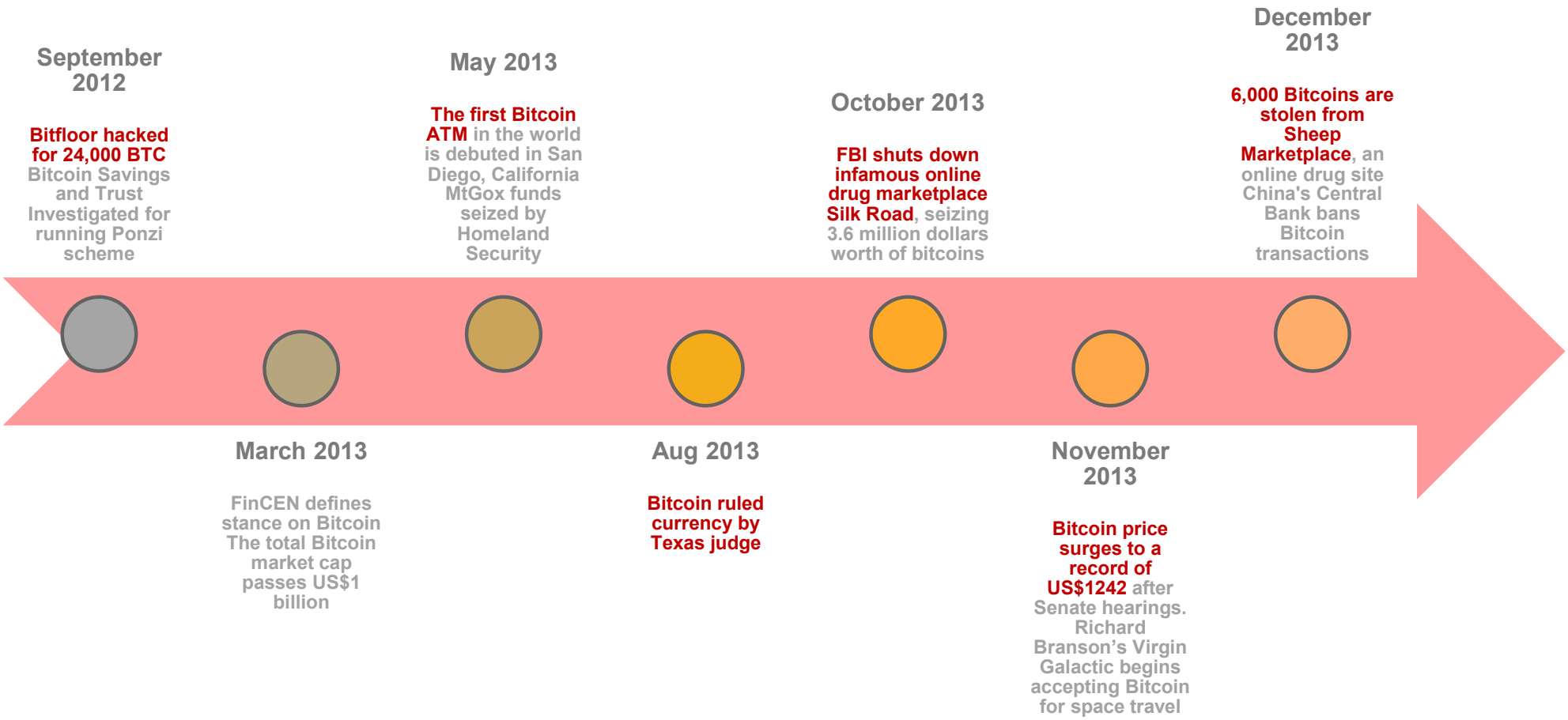
History of Bitcoin – Initiation



History of Bitcoin - Growth



History of Bitcoin – Growth



Let's talk about….

The Rise of Blockchain

- Financial Crisis of 2007-08
- Bitcoin – How it started

Blockchain Technology Today

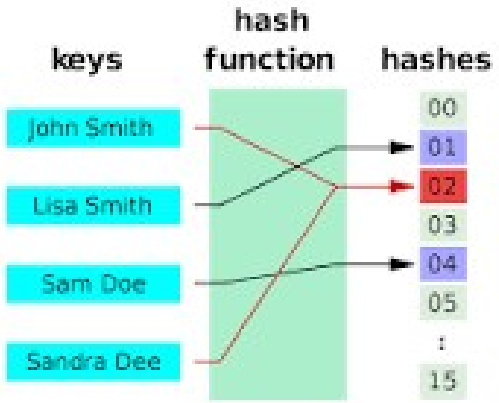
- Bitcoin – The inner working
- The Underlying Principles
- The Technology / Platform
- Blockchain Benefits

Satoshi Nakamoto – How Bitcoin would work

A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending.

Huh??? Hashing?

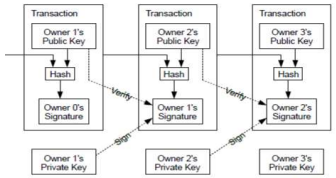
Hash function



Satoshi Nakamoto – How Bitcoin would work – 9 Key Elements

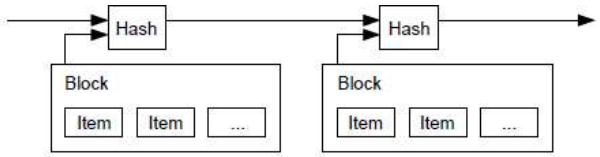
A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution

Transactions



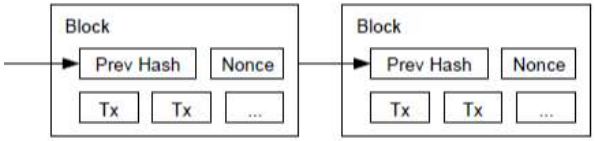
An electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.

Timestamp Server



A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post [2-5]. The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash.

Proof-of-Work



The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash.

Network

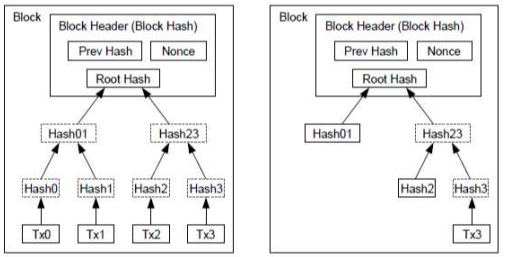
Steps to run the network -

1) New transactions are broadcast to all nodes.
2) Each node collects new transactions into a block.
3) Each node works on finding a difficult proof-of-work for its block.
4) When a node finds a proof-of-work, it broadcasts the block to all nodes.
5) Nodes accept the block only if all transactions in it are valid and not already spent.
6) Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

Incentive

The first transaction in a block is a special transaction that starts a new coin owned by the creator of the block. This adds an incentive for nodes to support the network, and provides a way to initially distribute coins into circulation, since there is no central authority to issue them The steady addition of a constant of amount of new coins is analogous to gold miners expending resources to add gold to circulation

Reclaiming Disk Space

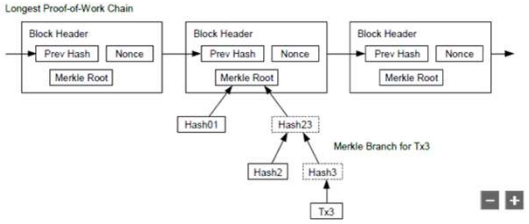


Once the latest transaction in a coin is buried under enough blocks, the spent transactions before it can be discarded to save disk space.

Satoshi Nakamoto – How Bitcoin would work

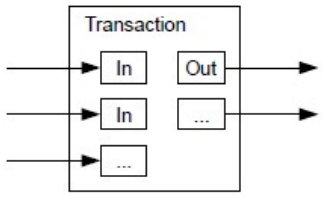
A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution

Simplified Payment Verification



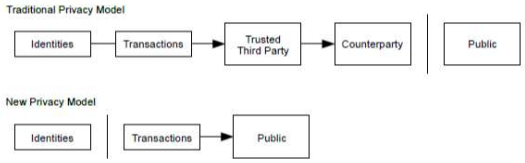
It is possible to verify payments without running a full network node. A user only needs to keep a copy of the block headers of the longest proof-of-work chain, which he can get by querying network nodes until he's convinced he has the longest chain, and obtain the Merkle branch linking the transaction to the block it's timestamped in

Combining and Splitting Value



To allow value to be split and combined, transactions contain multiple inputs and outputs. Normally there will be either a single input from a larger previous transaction or multiple inputs combining smaller amounts, and at most two outputs: one for the payment, and one returning the change, if any, back to the sender.

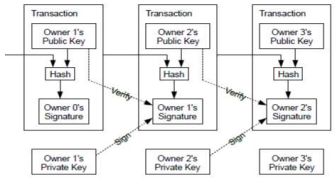
Privacy



The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone.

1. Transactions

Transactions



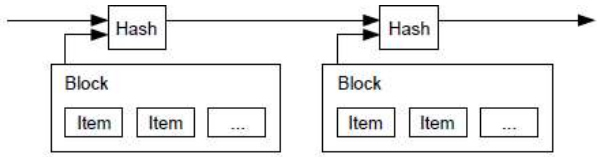
An electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.

A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution

Trusted Central Party / Mint

2. Timestamp Server

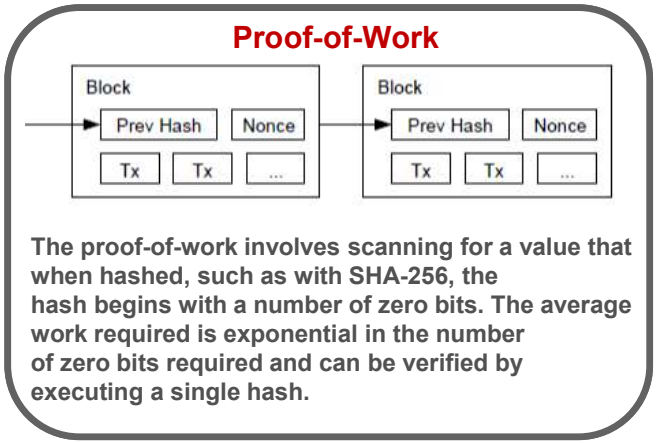
Timestamp Server



A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post [2-5]. The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash.

3. Proof-Of-Work

To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof-of-work system similar to Adam Back's Hashcash [6], rather than newspaper or Usenet posts. For our timestamp network, we implement the proof-of-work by incrementing a nonce in the block until a value is found that gives the block's hash the required zero bits. Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work. As later blocks are chained after it, the work to change the block would include redoing all the blocks after it.



4. Network

Network

Steps to run the network -

1) New transactions are broadcast to all nodes.
2) Each node collects new transactions into a block.
3) Each node works on finding a difficult proof-of-work for its block.
4) When a node finds a proof-of-work, it broadcasts the block to all nodes.
5) Nodes accept the block only if all transactions in it are valid and not already spent.
6) Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

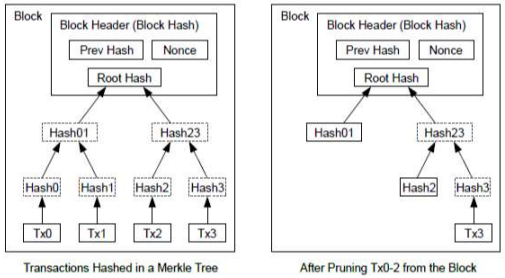
5. Incentive

Incentive

The first transaction in a block is a special transaction that starts a new coin owned by the creator of the block. This adds an incentive for nodes to support the network, and provides a way to initially distribute coins into circulation, since there is no central authority to issue them The steady addition of a constant of amount of new coins is analogous to gold miners expending resources to add gold to circulation

6. Reclaiming Disk-Space

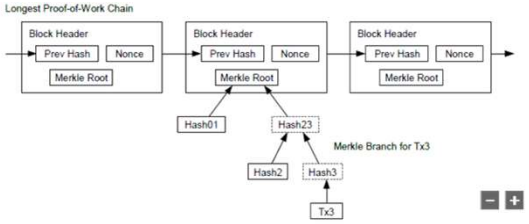
Reclaiming Disk Space



Once the latest transaction in a coin is buried under enough blocks, the spent transactions before it can be discarded to save disk space.

7. Simplified Payment Verification

Simplified Payment Verification

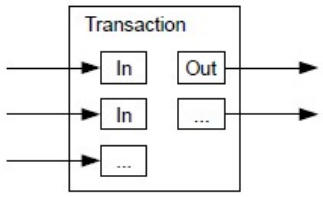


It is possible to verify payments without running a full network node. A user only needs to keep a copy of the block headers of the longest proof-of-work chain, which he can get by querying network nodes until he's convinced he has the longest chain, and obtain the Merkle branch linking the transaction to the block it's timestamped in

8. Combining And Splitting Value

It should be noted that fan-out, where a transaction depends on several transactions, and those transactions depend on many more, is not a problem here. There is never the need to extract a complete standalone copy of a transaction's history.

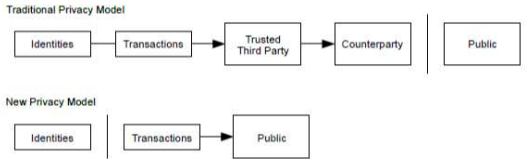
Combining and Splitting Value



To allow value to be split and combined, transactions contain multiple inputs and outputs. Normally there will be either a single input from a larger previous transaction or multiple inputs combining smaller amounts, and at most two outputs: one for the payment, and one returning the change, if any, back to the sender.

9. Privacy

Privacy



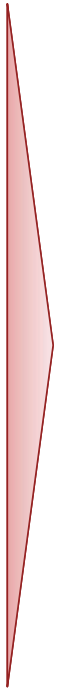
The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. This is similar to the level of information released by stock exchanges, where the time and size of individual trades, the "tape", is made public, but without telling who the parties were.

What is Blockchain?

A Next generation decentralized database…

"DLT" or "blockchain" denotes a shared digital ledger with **unique characteristics** –

- Eschews server-client model
- Each participant has its own copy of the database
- All changes are recorded, grouped into blocks, and verified by all peers
- This continuously-updated, tamper-proof database is called the blockchain



- ✓ **Decentralized** – no single point of failure
- ✓ **Smart contracts** – certainty of code execution
- ✓ **Only designated parties** have control of given data
- ✓ **Pseudonymity** – not anonymity
- ✓ **Public verification** – irrefutable timestamping
- ✓ **Forward-only** – unalterable, though not unamendable

….With a novel coupling of characteristics….

Why is it interesting

…. Yielding a singular value proposition

Decentralized network

In brief, blockchain offers a new model of verifiable trust –

- A single, immutable source of truth, with no single point of failure
- Existing across trust boundaries over any business network

Centralized network

By contrast, the status quo depends on trusted intermediaries running centralized databases -

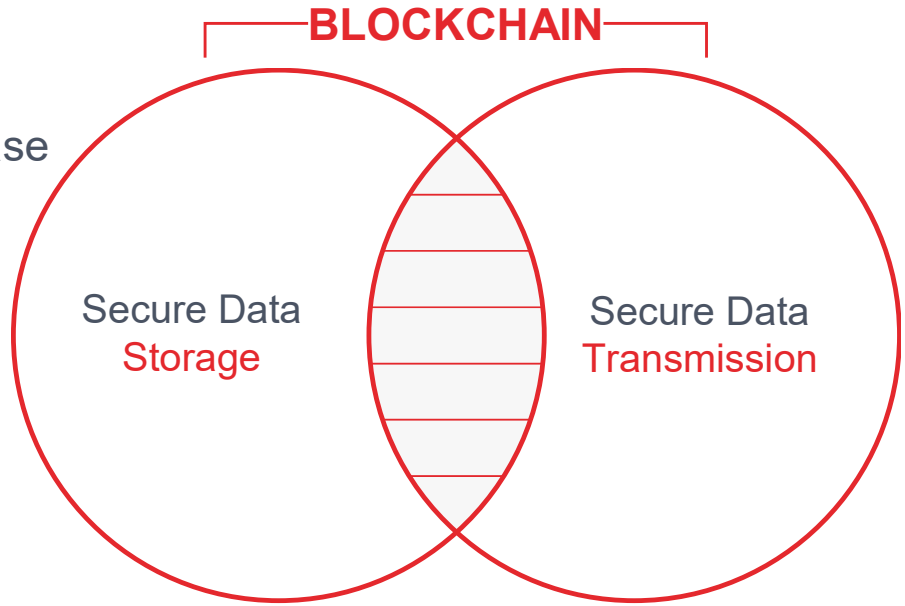
- Single points of failure
- Complicated & costly - reconciliation, communication, security, et al.

Blockchain is the Enabler of…

1. Financial Assets; or
2. Transactions; or
3. Contracts; or
4. Agreements; or
5. Any Functionality Requiring a Secure Decentralized Database

Real Assets

Debt



Blockchain - Distributed Ledger Technology

What is DLT?

Distributed Ledger Technology, or blockchain, is a **new form of decentralized database**.

Strong cryptography ensures only designated parties can modify data held on the network.

Data is chunked into "blocks" that are "chained" together, giving the technology its name.

Why is it interesting?

The technology enables a series of technology **breakthroughs directly applicable to today's financial markets**:

- Single truth
- Immutability
- Strong data governance
- Streamlined operations

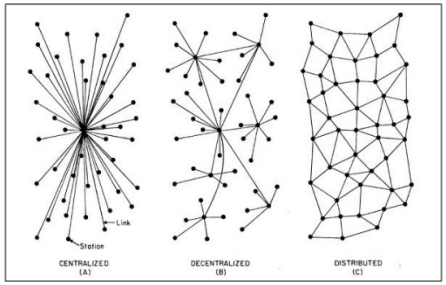
How does it work?

The technology itself is **configurable per business needs**, and is at its core an efficient bundling of several well-known, time-tested concepts in computer science:

- Peer-to-peer networking
- Public key cryptography
- Distributed consensus

How does it Work? Three key computing concepts

Peer-to-Peer Networking



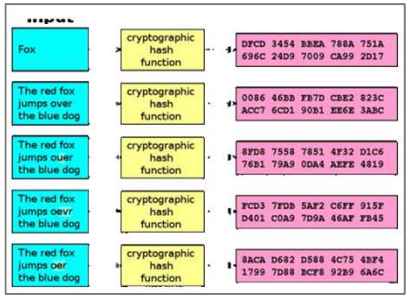
Distributed network architecture undergirds blockchain:

- Peers are equally-privileged participants
- Popular examples of p2p systems include git, BitTorrent, or Bitcoin
- Solves "synchronization" problem in trustless environment

To reiterate: status quo is client-server model

- Single points of failure
- High-cost and complication

Public Key Cryptography



Cryptographic Hashing

- Takes an input ('message') and returns a fixed-size output ('digest')
- One-way functions - easy to determine output from input, yet extremely hard to determine input from output

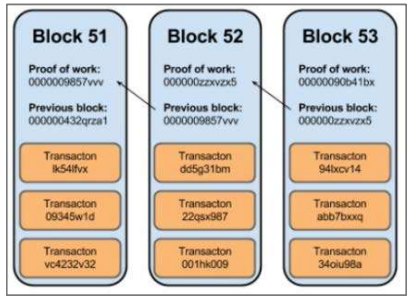
Public & Private Keys

- Message encrypted with a recipient's public key can only be decrypted by the recipient's private key

Digital Signatures

- Authenticity of a message signed with sender's private key can be verified (but not accessed) by anyone who has the sender's public key

Distributed Consensuses



Means by which network comes into agreement ('achieves consensus') about: [1] the global state of the database; & [2] veracity of additions thereto -

- Rules are baked into the protocol
- All blocks include a hash reference to the previous block – creating immutable chain
- Termed 'mining' or 'confirming blocks' in public ledgers

Different consensus mechanisms are optimized for different environments and use cases, e.g. -

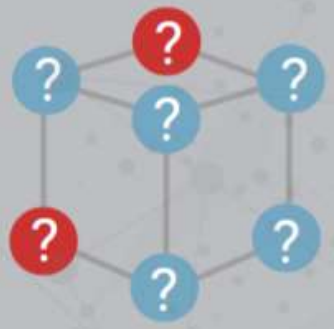
- Proof of Work (PoW)
- Proof of Stake (PoS)
- Proof of Elapsed Time (PoET)

Concepts in Action - Sample Transaction

	User Activity	Network Activity	
1	**Alice** has a balance of 10 Tokens wants to send 1 Token to Bob – the Token may represent a loyalty point or a financial product.	Both Alice and Bob have a **public key** (or 'wallet address,' which acts as the **pseudonym**), as well as a secret **private key.**	Only appropriate parties have access to modify the underlying data
2	Alice submits a message to the network, granting Bob access to a 1 Token balance.	Alice's message is signed with her private key and encrypted with Bob's public key. Only Bob can access the message / spend the Token. Yet the entire network can verify from **the output** that Alice (and no one else), was the signatory.	All messages are protected by strong cryptography
3	The message / position update is then broadcast to the entire network.	The message is relayed from node to node rapidly by **equally privileged peers** across the entire **peer-to-peer network**.	Messages are broadcast across the entire network
4	Transaction processors verify the message, and include it in the latest block – Alice's transaction is now **confirmed**.	Transactions, if valid, are included in the new block, along with a reference to the previous block, ensuring the immutability of all prior blocks.	The network comes into agreement on "global state"

Distributed Ledgers

Public Blockchain



Ledger is **fully open to public participation**. All users and and transaction validators are pseudonymous.

Federated Blockchain

Ledger remains open to public access, **but transactions are validated by known parties**.

Permissioned Blockchain

Ledger access is restricted to positively identified users. **Most appropriate for high-value, sensitive markets and assets.**

Ownership vs. Activity Ledgers

	"Asset Ownership Tracking"	"Activity Register"

What is being tracked?	• Changes of ownership of digital tokens
	• Tokens may be actual assets (e.g. BTC, XRP)
	• Tokens may also represent claims
		• Immutable timestamped data records
		• Underlying data can be anything -
		  ▪ Trade Facts
		  ▪ Identity information
		  ▪ Newspaper headline
		  ▪ Picture

What does Consensus denote?	• Network agrees said ownership changes are valid as per network rules • Network stores changes in ownership	Two categories for consensus - • **Relevant party consensus**, i.e. one or more parties agree on the content of some data • **Network consensus**, i.e. validating parties agree that the existence of data has been legitimately uploaded

Blockchain – Key Benefits

This system of organizing and storing information ensures a number of benefits

Immutability

- This system of organizing and storing information ensures several benefits.
- Since multiple copies of a block chain are kept and managed by consensus across a peer-to-peer network, no one peer can alter past transactions.

Security

- It is a fundamental cryptological law that it is relatively easy to set a problem that is very, very difficult to solve.
- What is relatively easy for a network of computers to do is, in practice, impossible even for much larger networks to undo.

Verifiability

- The combination of transparency and immutability also allows us to satisfy full public verifiability: anyone in the world can check for themselves that the rules of the system - in the case of digital currencies, that coins should be spent only once -are being followed.
- Whilst information cannot be manipulated, it can be easily verified thanks to the size and power of the network.

Resilience

- The distributed nature of the ledger makes it resilient. Even if many peers go offline, the information is still accessible.

Transparency

- The fact that all transactions are broadcast to all peers also makes the ledger transparent.
- However, the encrypted nature of the transactions means that privacy is also assured.

These benefits can be tuned and block chains tailored to their specific functions to ensure that issues such as privacy accountability, and transparency are tightly managed.

What are Crypto Networks and Why are Tokens Fundamental?

Crypto Networks are Internet 3.0

Crypto Networks are decentralized networks built on top of the internet that provide a wide variety of digital services, such as data storage, computation, and interactive applications.

They are to today's centralized internet applications (Google, Facebook, Amazon, etc.) what the original internet was to Prodigy and CompuServe.

Tokens are integral to how crypto Networks work

Tokens (also known as cryptocurrencies or crypto Assets) are the internal currency of crypto Networks, and the incentive mechanism which enables them to function. Tokens can have properties of currencies, commodities, and securities.

For crypto Networks to function, tokens must be distributed widely among network users and participants.

Definitions

"Public" or "Open" Networks

● Open source and "forkable": the network's entire source code is available under an open license, therefore anyone who wishes to can run a competing copy.

● Open to all participants: anyone who wants to join the network can operate a node that provides the network service -- as opposed to so-called "permissioned" networks where access is gated.

PRIVATE or PERMISSIONED Networks are just that – limited to a private group or require permission to join. E.g. Enterprise Applications

"Utility" vs. Investment Function

Some crypto Networks and their associated tokens are expressly designed to function like investments -- meaning, they have explicit profit-sharing or asset ownership functionality.

An Ecosystem – Not a Company

Like the original internet, each crypto Network is an ecosystem, not a company.

While a crypto Network may initially be designed by a single group or company, ultimately the participants (often known as “miners”, though there are other roles in some crypto Networks, such as “validators”) are independent actors, each running a copy of the network’s open source software to provide the digital service.

Typically, each crypto Network has its own internal cryptocurrency or token which serves many purposes within the network. Tokens serve as the internal currency, provide an incentive for the supply-side to provide the service, are often part of the network’s “governance” process, play a role in the network’s security model, and more.

Decentralized

Decentralization is the critical architectural element of cryptonetworks, because, like the architecture of the original internet, it offers:

● Innovation: by design, crypto Networks are open to all innovators. We can expect a wave of innovation similar to the birth of the internet. ● Competition: crypto Networks are a natural hedge against concentrated market power in the tech and finance sectors, due to their open source and “forkable” architecture -- imagine being able to “fork” Google or Amazon and make your own copy.

Crypto Networks also provide new functionality, including: ● Data integrity & security: crypto Networks provide an immutable ledger (often called a blockchain) for storing data, which can’t be manipulated by any single party. This alone is a foundational innovation with wide applicability across sectors.

Tokens provide the incentive mechanism for these decentralized, independent actors to work together to provide the network service.

Consensus

The key innovation of crypto Networks is the ability to come to consensus on the “state” of the data, despite the absence of a central controlling party.

There are many approaches to achieving consensus, including “proof of work” (solving a complex mathematical puzzle), “proof of stake” (risking your tokens), “proof of space-time” (verifying file storage), and many others.

Importantly, the consensus process ensures that every token is a “scarce” asset and that the distributed ledger of token transfers (often, a blockchain) is always up-to-date and accurate -- this is what gives tokens real value.

Each network’s ledger is also effectively a database where other kinds of data can be securely and permanently stored.

Despite the absence of a single controlling party, network participants can come to consensus on the state of data, and record it, immutably, in a distributed ledger, or blockchain.

Tokens are central to the consensus process, as they provide incentives for participating, and play other key roles, especially in “proof of stake” networks.

Governance

Since each crypto Network is an ecosystem of independent participants, the process of technical and policy decision-making, known generally as governance, differs significantly from that of a traditional technology company that can make unilateral decisions.

An “open” or “public” crypto Network is run on open-source code that anyone can copy, or fork, in order to run a competing network. Above all else, the ability to fork a crypto Network and create an identical working copy provides a strong set of checks and balances in the governance of the network.

Imagine, for example, that if Amazon’s or Google’s users & investors didn’t approve of the company’s decision-making, they could a make a perfect copy and launch a direct competitor -- this is the dynamic within crypto Networks.

Tokens can also play a role in the governance process, for example via holding or “staking” tokens as part of participating in governance.

Central Role Of Tokens

As we have seen in the previous slides, the token is what ties the entire crypto Network together.

For each crypto Network, the token acts both as the internal currency (users spend it to use the service) and the incentive to provide the service (miners and other participants earn tokens in exchange for providing the service), and also plays an integral role in the consensus, security and governance processes of each crypto Network.

Finally, because users of the network are also holders of the tokens, crypto Networks have the potential to distribute network value broadly to all stakeholders (next slide).

users pay in tokens to use the service

some tokens are used elsewhere in the protocol, e.g., for “staking” or as part of the governance process

users purchase tokens for use on the network

miners/participants earn tokens for providing the service

Tokens are central to many aspects of the operations of crypto Networks, playing a variety of functional roles.

Broad Alignment and Special Incentives

Because network participants (miners, validators, committee members, as well as individual users) earn tokens as they work to provide the network service, and as tokens generally become more valuable the more useful a crypto Network becomes, all network participants are aligned to make the network more functional and therefore more valuable.

In this way, cryptonetworks offer a very different organizing model for providing network services, more like a mutually-owned company, a cooperative, or a credit union than like a traditional technology corporation. In summary: ● Cryptonetworks are a new model for providing internet-enabled digital services. ● They offer new characteristics, specifically increased innovation, competition, and information security, as well as direct economic incentives for all stakeholders. ● Tokens are integral to all aspects of their operation.

Launching a Crypto Network: Typical Workflow

Pre-Launch

An individual, group or company designs a new cryptonetwork, its digital service, and its internal token.

They may take investment in the form of equity financing, may pre-sell network tokens, or may require no outside capital at all (as was the case with Bitcoin).

Live Network

The network's source code is published, typically under an open source license that allows others to copy and modify it freely.

Other actors besides the original designers begin to operate "nodes" and play other roles in the network, including contributing to the codebase.

The network begins to operate, achieving consensus and producing a ledger or blockchain.

Tokens are distributed to users and other participants, typically earned as part of providing the network service (e.g., "mining") or granted as part of an "airdrop" or giveaway to seed the network.

The token acts as the internal currency and incentive mechanism, and plays a role in other processes.

Tokens may begin to trade on third-party exchanges.

Utility or Security?

US Regulatory Test

Utility tokens give holders access to a specific protocol or network, oftentimes enabling them to use an associated product or service. With utility tokens, no ownership rights to the underlying company behind the associated product or service are granted to token holders.

Security tokens grant holders ownership rights to an underlying asset. In essence, they are asset investments governed by the protocol set forth by the associated blockchain

The Howey Test. If a token (or another instrument) meets all of the following criteria, the SEC considers it an "investment."

1. The user is investing money.
2. The user expects to profit from the investment.
3. The investment is in a "common enterprise."
4. Any profit comes from the efforts of a third-party or promoter.

Smart Contracts: Asset Ownership vs Activity Tracking

A smart contract is a computer program or a transaction protocol which is intended to automatically execute, control or document legally relevant events and actions according to the terms of a contract or an agreement.

A smart contract is a self-executing contract with the terms of the agreement between buyer and seller being directly written into lines of code. The code and the agreements contained therein exist across a distributed, decentralized blockchain network. The code controls the execution, and transactions are trackable and irreversible.

Smart contracts permit trusted transactions and agreements to be carried out among disparate, anonymous parties without the need for a central authority, legal system, or external enforcement mechanism.

While blockchain technology has come to be thought of primarily as the foundation for bitcoin, it has evolved far beyond underpinning the virtual currency.

Security Tokens / Smart Contracts - Overview

Diversification

Build bundled portfolios of assets

Access

24/7 Global Markets

Lower Risk

Less fraud, less tampering

Better Privacy

Protecting businesses and consumers

Smart Contracts

Automate dividends, voting, transfer

Transparency

The right information to the right people

Cost Savings

Streamline back-office processing

Efficiency

Faster processing or reporting