DAVID ANDREWS, FOUNDER
RYATTA GROUP, @RYATTAGROUP

BLOCKCHAIN FOUNDATIONS

- cryptography is defined as
  the practice and study of techniques for secure communication

- in the early days this was accomplished through mechanical means such as the Lorenz or Enigma cipher machines from World War 2 or human means like the ciphers team at Bletchley Park in England

- with more powerful general purpose machines and blossoming opportunity, cryptography has expanding into a more general pursuit, not strictly limited to encryption
- deriving from the disciplines of mathematics, computer science and electrical engineering it has become

- the chip in your credit card is a good example of cryptography in practice
- secure connections on the web (SSL or HTTPS)
- Blockchains rely heavily on cryptography to support data integrity and non-repudiation

- a basic and useful operation found in cryptography is the cryptographic hash function

- given an input, the cryptographic hash produces a unique fixed-length value as output
- the output, called a hash value, is a summary of the input
- this summary is often used to ensure the input has not been modified, kind of like a fingerprint, but the cryptographic hash is sensitive to every part of the body of the input rather than the pattern in a small part of the input
- perhaps a better analogy is to say the hash function boils down the content - distills it into a syrup that is smaller than the original, yet somehow still represents it

- Suppose we used a cryptographic hash function to summarize an email
- based on the email, the hash function summarizes or computes a hash value that is a short fixed-length value
- given an email, and the hash value computed with it
- if a letter in the email were capitalized -> the hash would change
- characters were switched, say ‘creative’ to ‘reactive’ -> the hash would change
- even if a space is added or removed -> the hash would change

- The hash gives us a simple way to tell if the email changed, without storing and comparing the old and new versions of the email - a summary of the contents without the contents themselves
- obviously we need to guarantee a hash function will return the same result given the same input - otherwise we would have false positives when checking for content changes

- the output of a cryptographic hash is composed of the entirety of the document content but in a form that makes it difficult to reconstitute the original - this is not quite a perfect analogy since the volume of ground meat is the same as the input (whereas a hash is a “digest” or boiled down version), but the mixing of different parts of the input and the non-reversibility of the operation (for instance, you can’t put the steak back together) are fairly represented

-

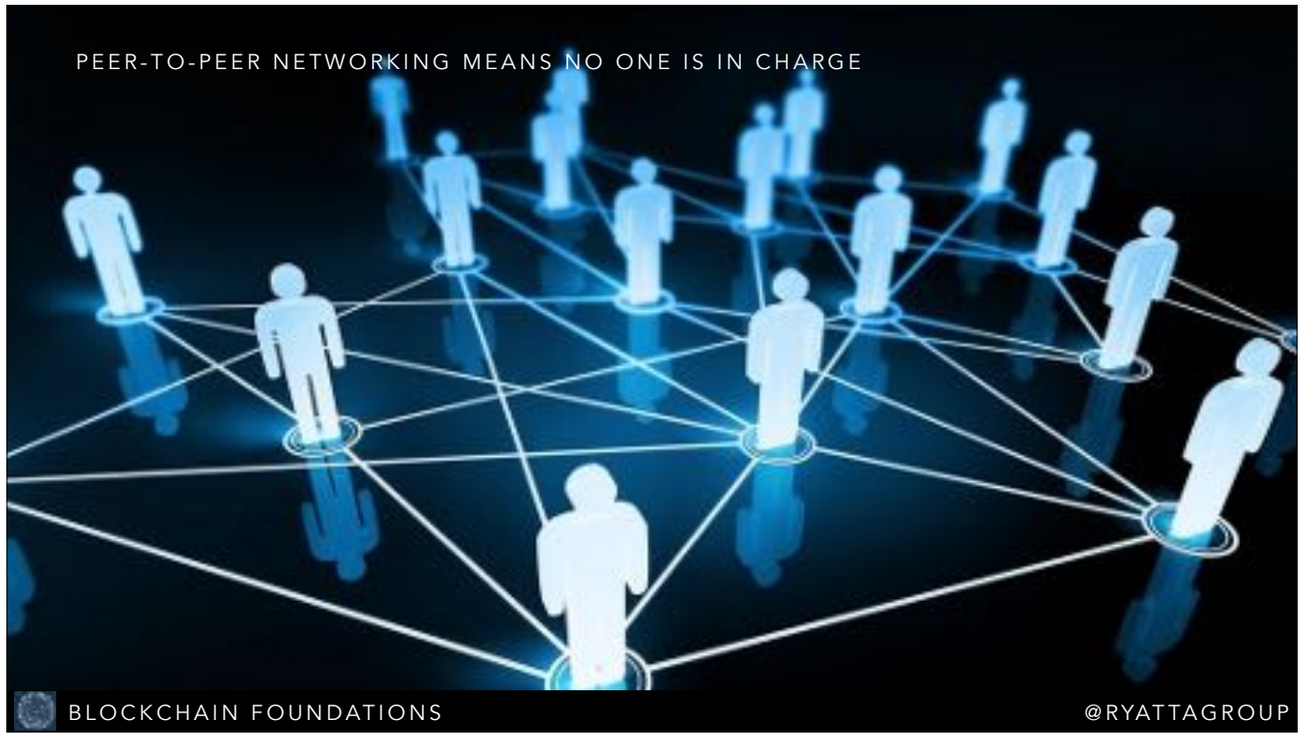
- imagine a Wooden box
  with pair of locks admitting two different keys

- the box can be locked with either key
  but locks work together such that
- once locked it requires the other key to unlock

- suppose I give you the bronze key, we can securely exchange things using the box
- if I receive the box locked,
- I open it with my gold key
- I take out contents, if any
- place new items in the box
- lock it with my gold key
- I return it to you to repeat the process

- this is an analogue for a cryptographic process called public key cryptography

- the two keys have a relationship that has two interesting features:
- one key can easily decode messages encoded by the other (akin to unlocking the box), and it is practically impossible to determine the private key given the public key
- when you receive the box, you can be certain that it was me who locked it - the converse is not true since anyone can have the public key



- A peer-to-peer network is a distributed architecture that partitions tasks or work loads between peers, where each are equally privileged
- peers are both a client and a server (meaning they both consume from, and provide services to, the network)
- peers can collaborate on any type of task
- the most common task has been file-sharing
- the first popular instance of a peer-to-peer network was the music-sharing application Napster, released in 1999, allowing millions of people to collaborate to share, locate and download music files
- but USENET, a lesser-known but similarly decentralized message distribution platform, was developed 20 years earlier and continues to run today, perhaps because of its relative obscurity

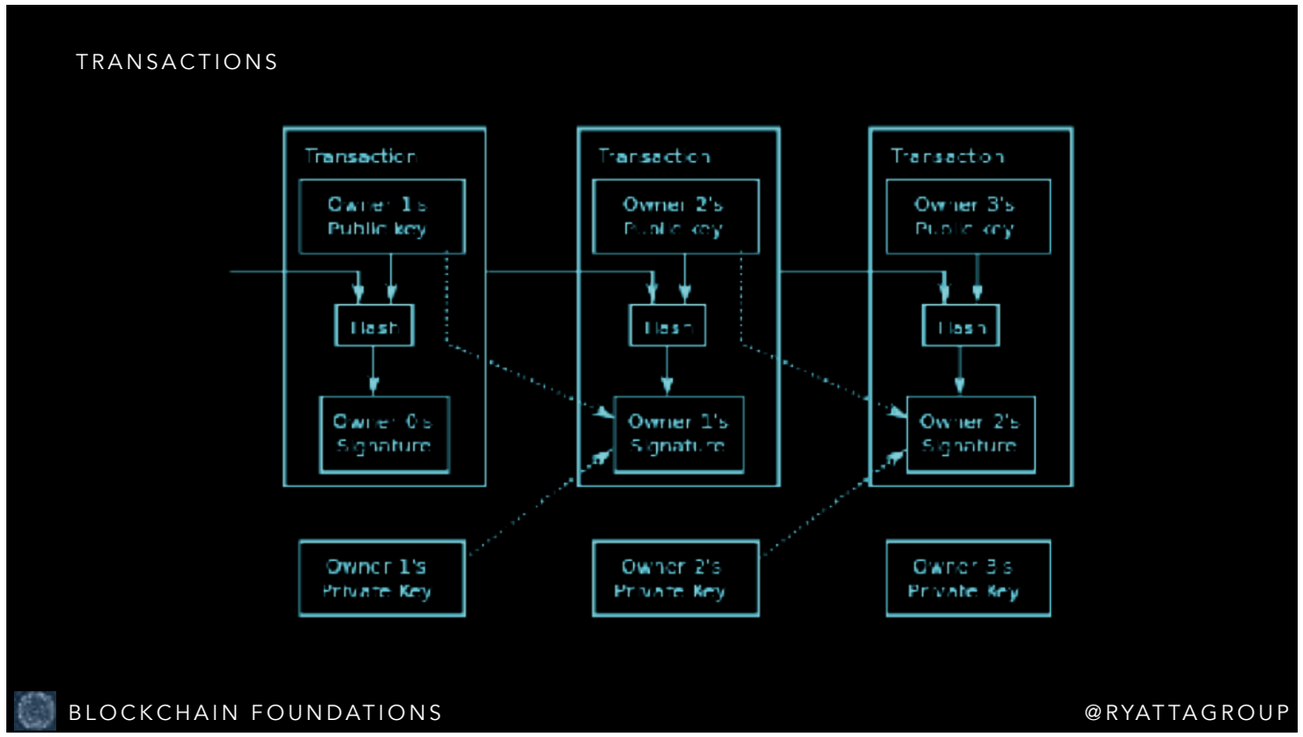
Benefits of a peer-to-peer network are:

- they are easy to join and leave, peers are connected to multiple producers and consumers
- no central point of failure, shutting down any given node affects the network operation very little
- a document will be held by many or all peers on the network, the removal of any given node will affect the availability of a document very little

- because of these traits, a peer-to-peer network with sufficient peers is said to be “unstoppable”
- to stop the network would require removal of all peers which, given the diversity of peers in many regards (political, geographic, technical, etc.) would be impossible

SATOSHI NAKIMOTO, THE SHADOWY FIGURE BEHIND BITCOIN

- On October 31, 2008 an unknown author using the pseudonym Satoshi Nakamoto posted a whitepaper to the cryptography mailing list hosted by Metzger, Dowdeswell, a New York-based networking and security company.
- It describes how to use hashing, public key encryption and peer-to-peer networking to create a new type of payment system, one which is entirely digital but provides many of the benefits of cash - a new type of currency for the digital age
- The motivation for doing this is disruption - to remove the inefficiencies inherent in now-dominant trust-based systems of the banks, the credit card companies and services such as Paypal



- An e-coin is defined as a chain of digital signatures, each transferring ownership of the coin to the next owner
- The current owner, Owner 1 in this diagram, transfers ownership to owner 2 by creating a transaction containing owner 1's signature and owner 2's public key
- Owner 1's signature is required to validate owner 1's authorization to "spend" the coin - this can be done using owner 1's public key, which is available in the current transaction
- The chain of signatures defines a continuous succession of owners for the coin
- Note that the input for the hash contains the previous block in addition to the new owner's public key - this guards against the transaction being replayed against another block or naming another owner as the recipient

- It could be second, minutes, hours, days, weeks or even years between these transactions.

THE CHAIN

MINING

USE CASES - CASH, CROSS-BORDER PAYMENTS, IOT, VOTING, DRM

ETHEREUM - THE BLOCKCHAIN ON STEROIDS

ETHEREUM USE CASES - SECURITIES SETTLEMENT

HYPERLEDGER - THE BLOCKCHAIN FOR BUSINESS

HYPERLEDGER USE CASES - SUPPLY-CHAIN TRANSPARENCY, SYNDICATED LOANS

THE FUTURE - NEXT STEPS

THE FUTURE - RISKS