DFINITY

The Internet Computer

Tonight we'll explore . . .

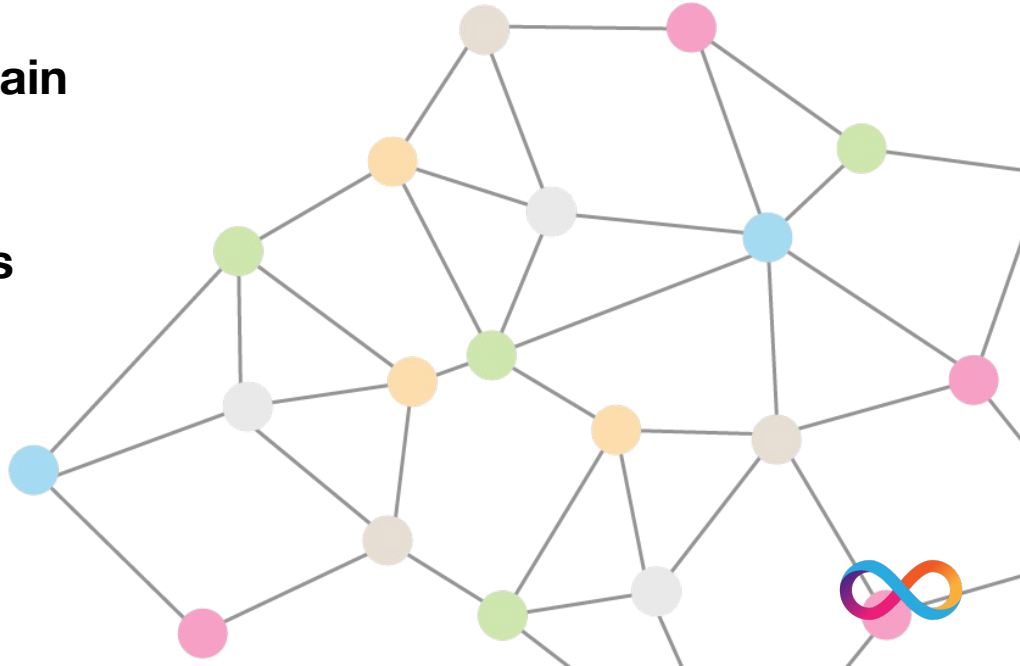
The need for a new global business and information infrastructure

The emergence of a new computing paradigm: WebAssembly & Cloud 3.0

Combining WebAssembly & Blockchain

The importance of randomness

How DFINITY generates randomness



DFINITY

The global information infrastructure is frail

The Problem: Hosting Logic & Data is A Pyrrhic Game

	Vulnerable to infrastructure failure	Vulnerable to data-theft	Vulnerable to data-harvesting	Business Dependency
Self-Hosted (owned infrastructure)	X	X		
Cloud-Hosted (AWS, Azure)	X	X		X
Outsourced (Global Payments, Gmail)	**X**	**X**	**X**	**X**

Black Elephants

2011: Human error during a system upgrade knocks out much of AWS service for 5 days

2012: Global Payments loses 1.5 Million credit card numbers

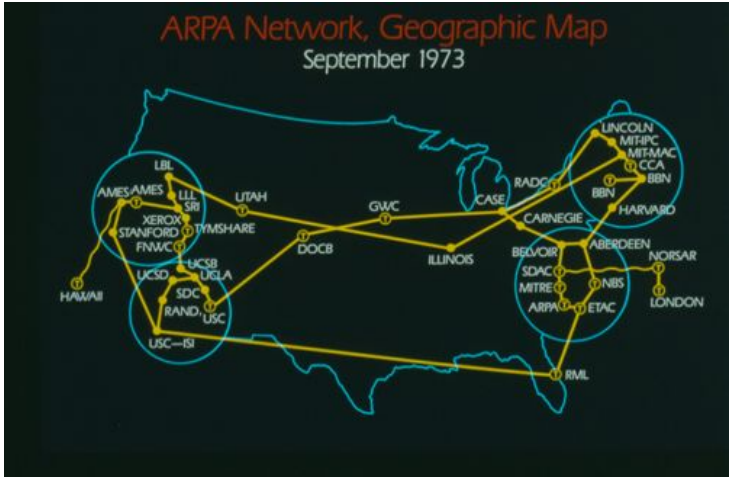
2013: Cambridge Analytica rears its ugly head

2016: Europe adopts the General Data Protection Regulation

2016: Storms in Sydney knock out AWS service for 10 hours

2017: Yahoo announces that in two hacks in 2013 and 2014 it lost 3 Billion usernames and passwords (everything)

2018: Maersk recovers from NotPetya ransomware incident by reinstalling over 4,000 servers, 45,000 PCs, over the course of ten days in late June and early July 2017.



SWIFT’s global business interoperation infrastructure is fragile

2015–2016 $101 million stolen in several attacks on Bangladeshi central bank and Vietnamese & Ecuadorian commercial banks.

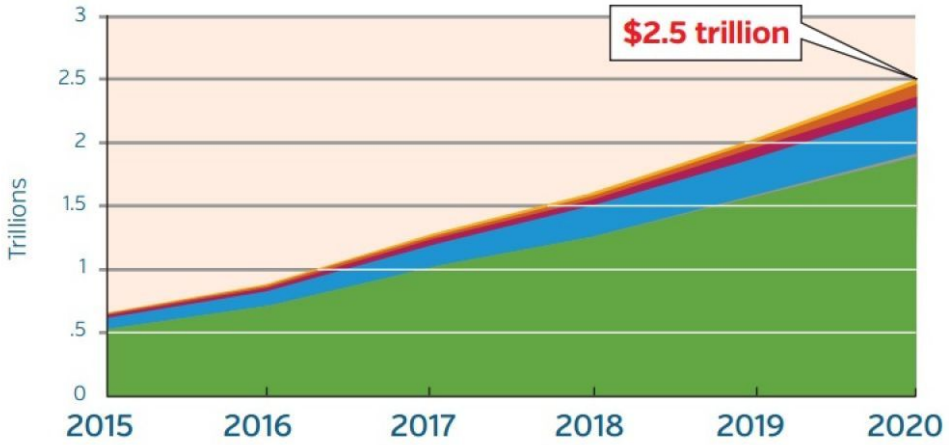
04/2017 We learn the NSA hacked SWIFT for surveillance purposes

10/2017 $61 million stolen from Taiwanese bank

Sometime in 2017 $6 million stolen in Russia bank attack

02/2018 $2 million Stolen from City Union Bank, Bangladesh

Worse by the year



A study conducted by Juniper Research has indicated that rapid digitisation of consumers' lives and enterprise records will increase cost of data breaches to approximately $2.5 trillion globally—almost four times the estimated cost of breaches in 2015.

We need a new Infrastructure

Does not fail due to ransomware

Is not controlled by gatekeepers

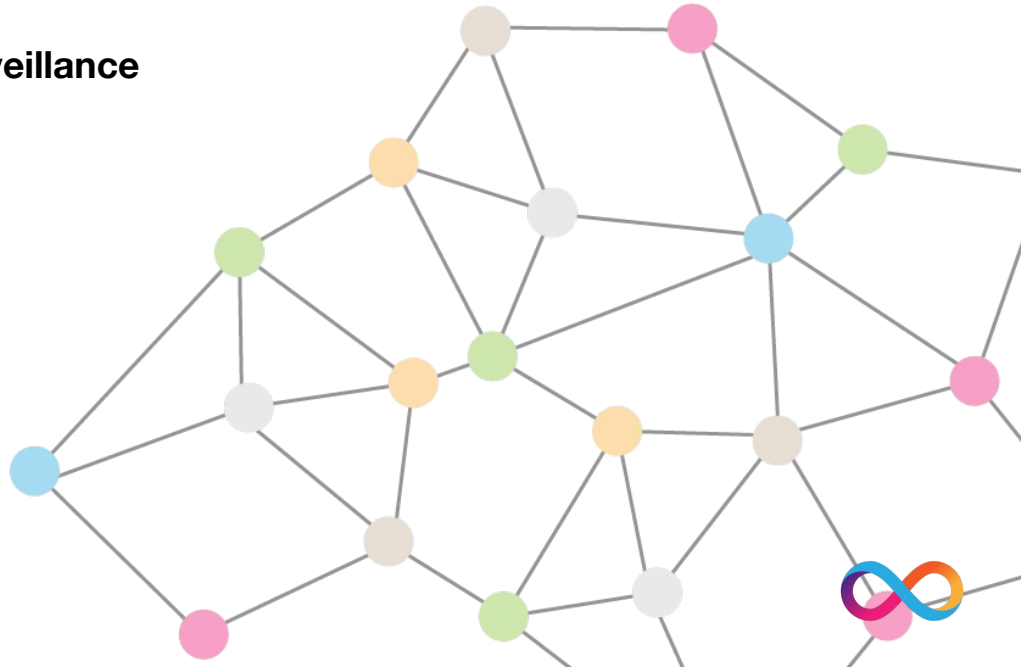
Won’t fail at any moment due to human error

Does not expose the user to data theft or surveillance

Cannot be manipulated by an attacker

Is structurally robust

Automated, Replicated, Decentralized



WebAssembly, Cloud 3 & Blockchain

WEBASSEMBLY

The next generation software development standard.

Allows one to program in the most appropriate language for an application

Can run on any computer or phone, currently in browser

Is sandboxed and deterministic

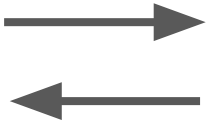
Cloud 3: Local + remote storage and execution in a single runtime environment

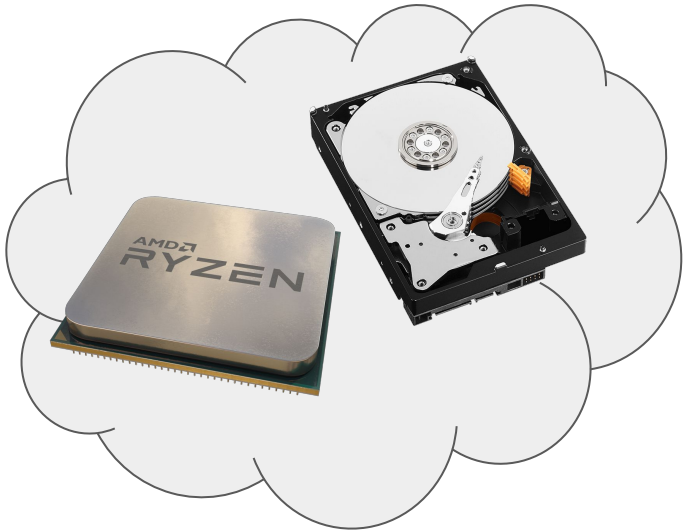
Interface downloaded to phone as application is opened.

Heavy storage and compute happens on cloud

Appropriate storage and compute happens on device.

Never update an app again

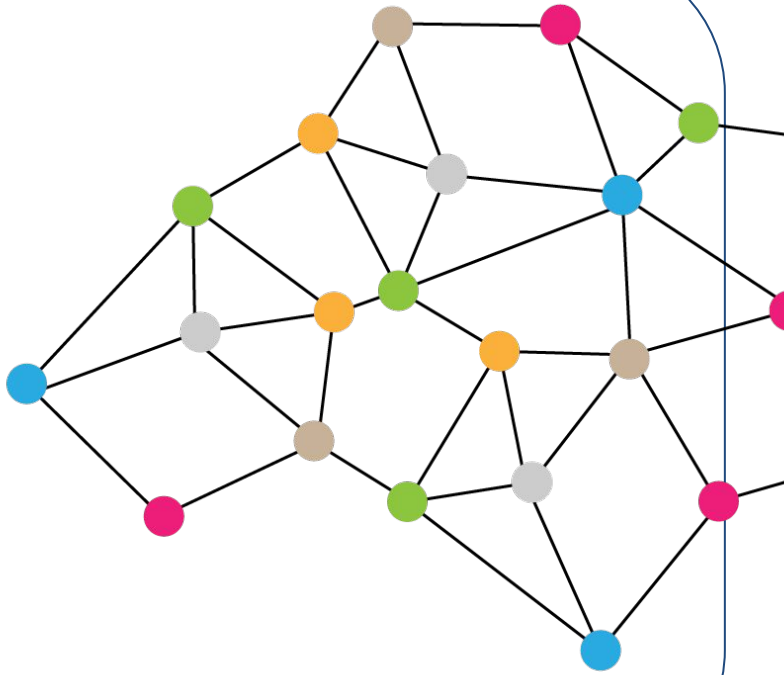




WASM + Blockchain: The Internet Computer

High security services requiring 100% uptime use a Blockchain for remote storage and execution.

High performance Internet Computer will be cheaper than centralized cloud due to lack of labour costs



The value of randomness

If we can agree that a source of randomness is

Unmanipulable

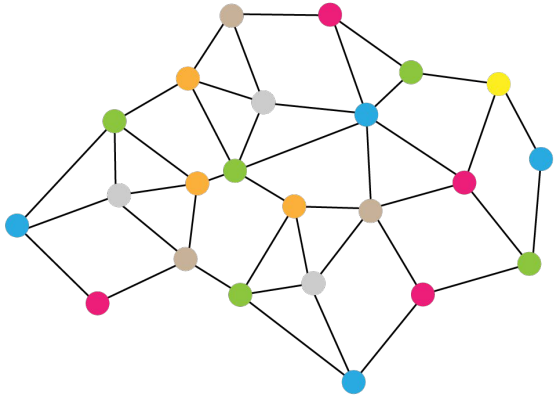
&

Unpredictable

We don’t need an expensive consensus algorithm to secure a distributed computing network.

This makes it cheap to run programs in this environment and easy to scale.

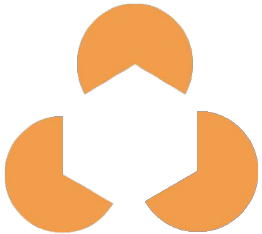
WEBASSEMBLY



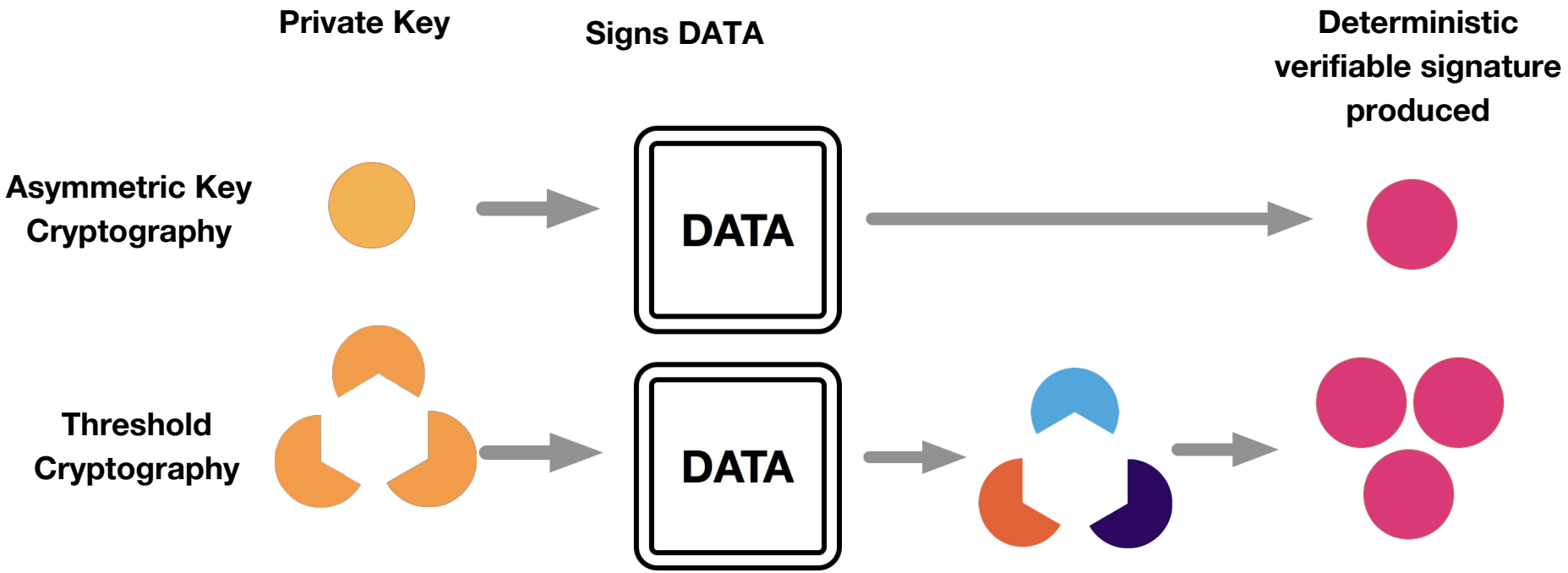
DFINITY

Generating Randomness

Threshold signatures 1

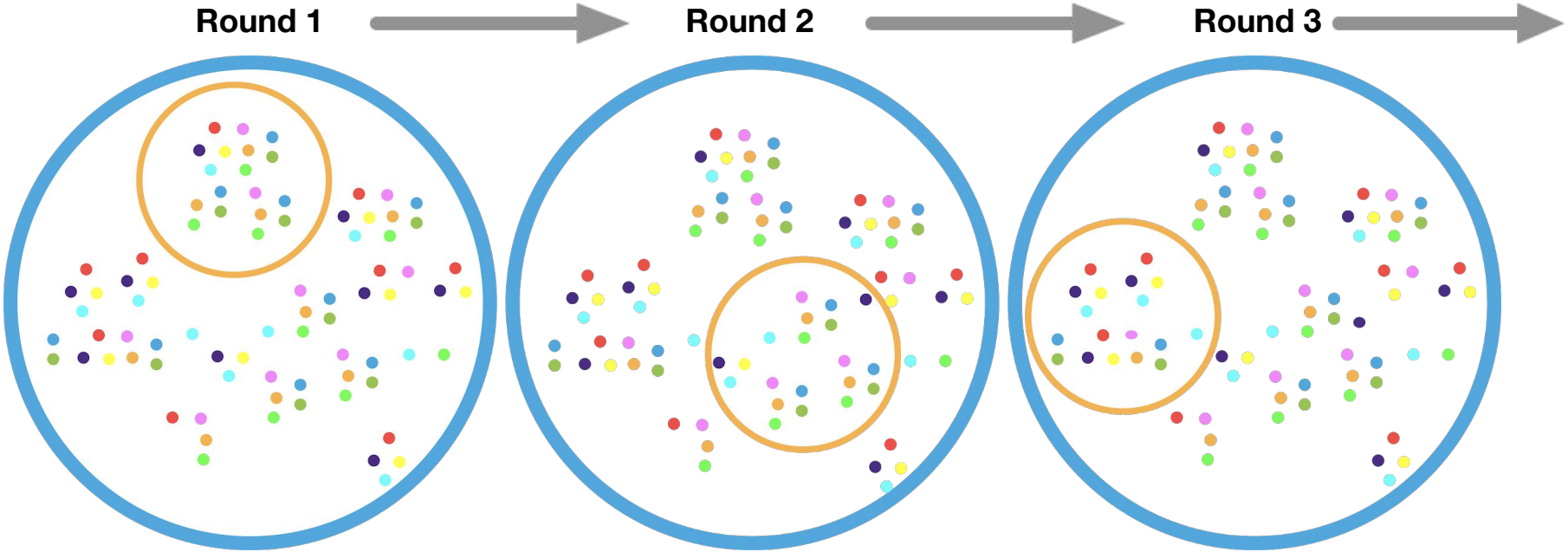
	Public Key	Private Key
Asymmetric Key Cryptography		
Threshold Cryptography		

Threshold signatures 2



DFINITY Consensus: Threshold Signatures and Notarization Committees

Each round, or block, a randomly selected **Notarization Committee** is selected to create randomness and notarize blocks for inclusion in the blockchain



DFINITY Consensus: Threshold Relay 1

Use **Randomness** to select **Notarization Committee**

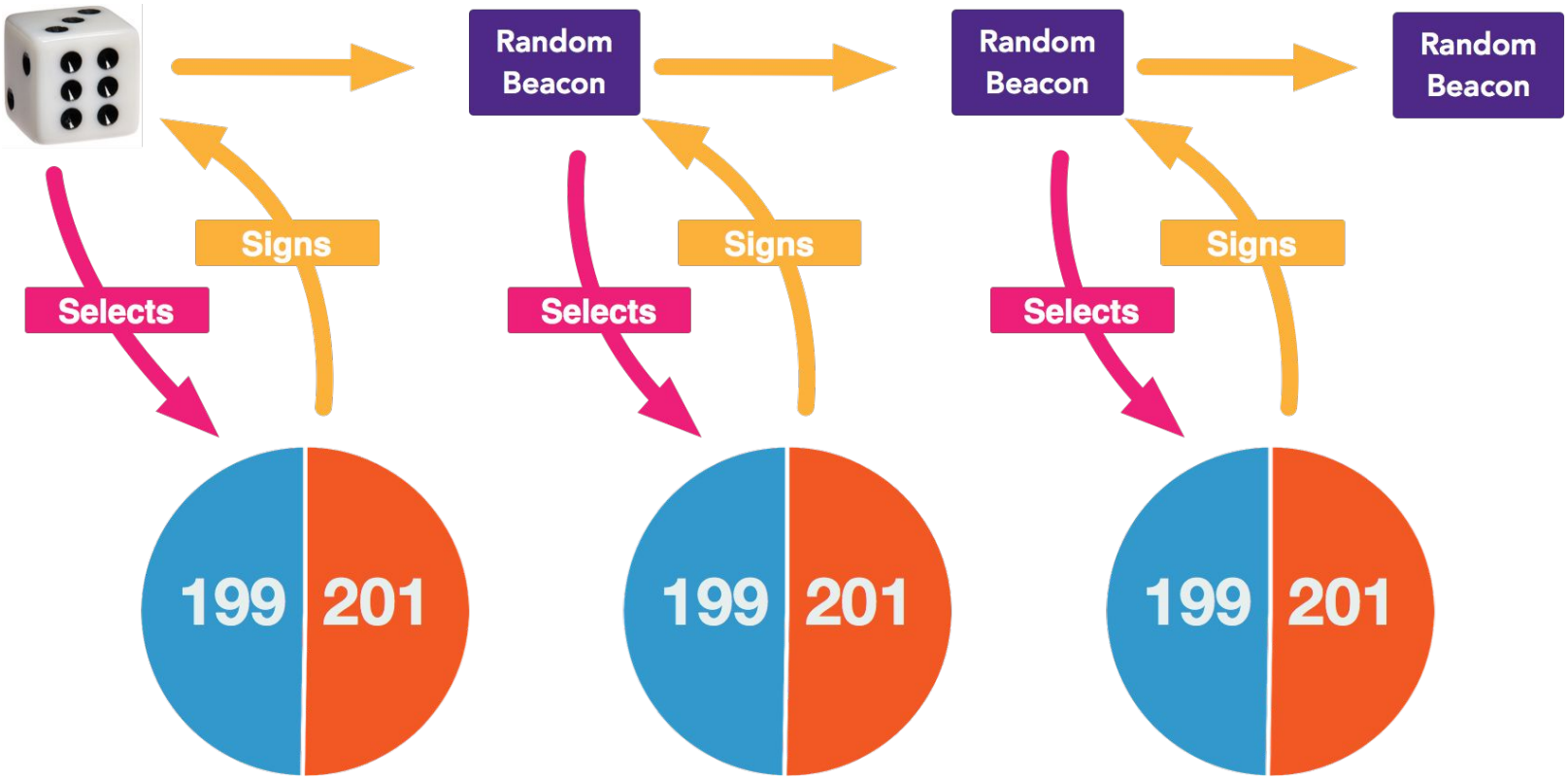
Committee runs **Distributed Key Generation Algorithm**

Committee members **sign the randomness that selected them**

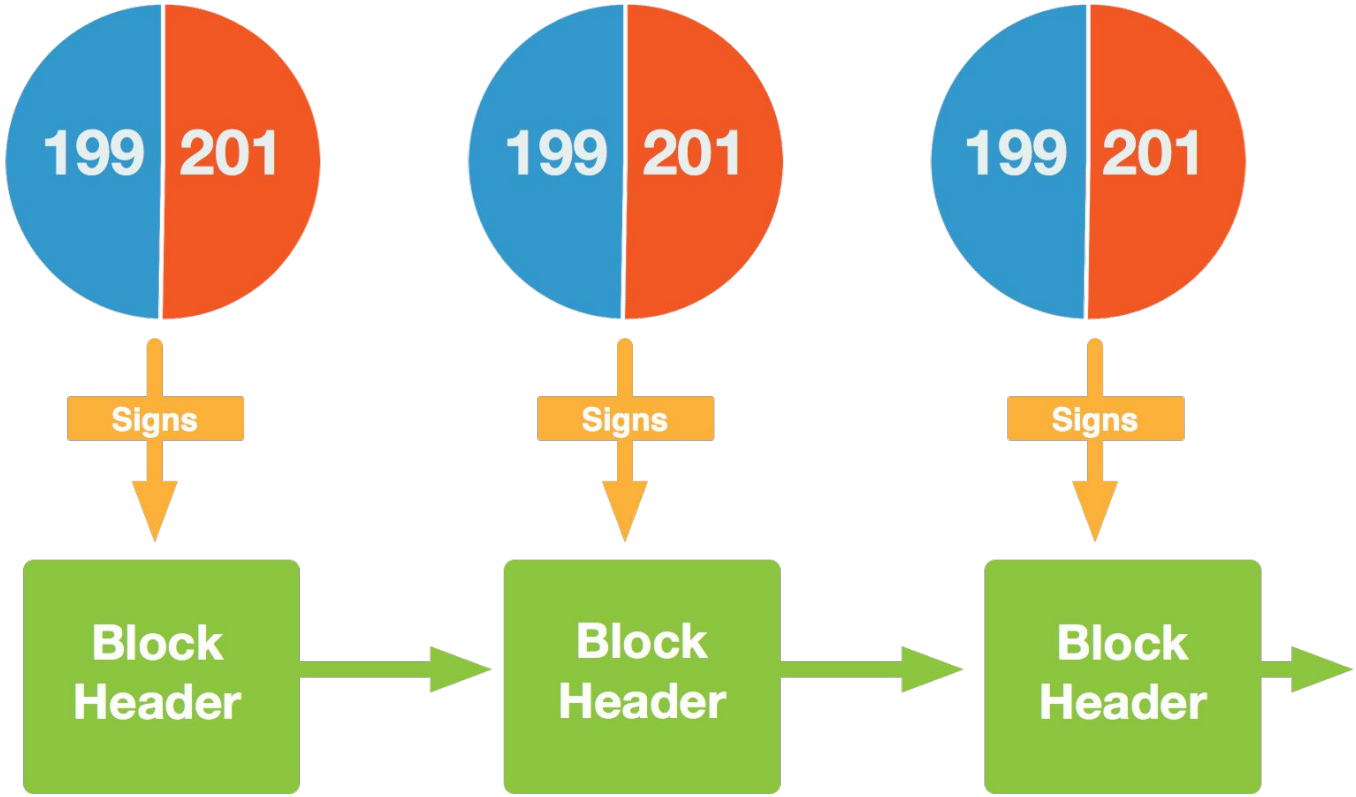
Signature shares are **gossiped onward and aggregated**

The **new complete signature** is used as randomness to **select the next Committee**

DFINITY Consensus: Threshold Relay 2



DFINITY Consensus: Block Signing




D I N I T Y
Network Dashboard
Contracts
DApps
Network
Recent Blocks
Random Beacon
Block Height
Latency Chart
seconds
169 800
170 000
170 200

DFINITY:

Cannot fail due to ransomware

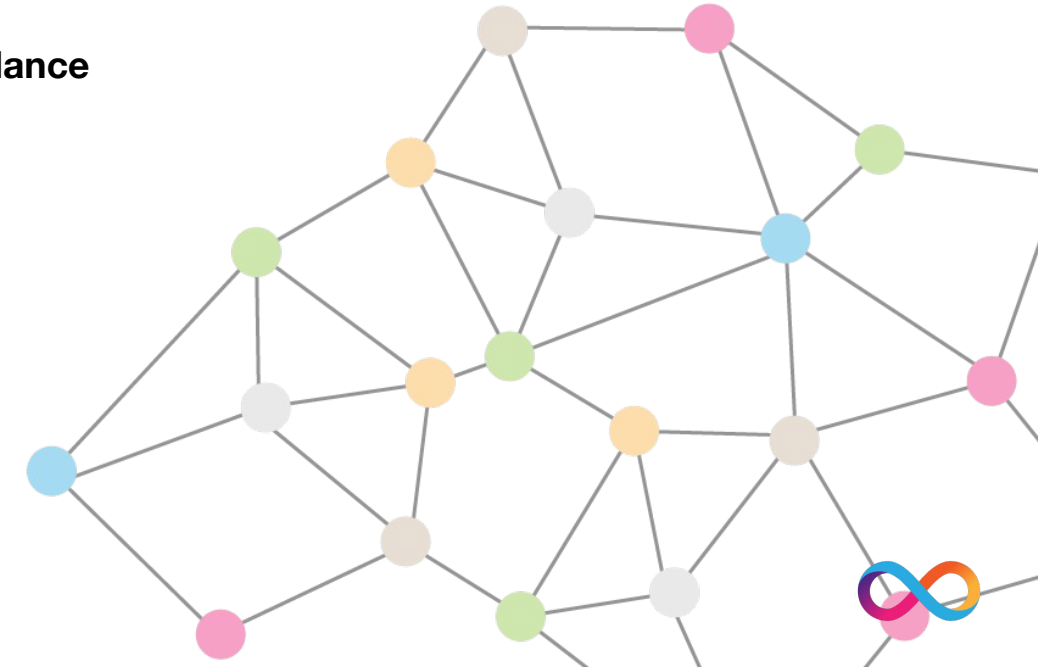
Is not controlled by gatekeepers

Won’t fail at any moment due to human error

Does not expose user to data theft or surveillance

Cannot be manipulated by an attacker

Is structurally robust



arthur@dfinity.org

DFINITY.org

DFINITY.org/jobs

@ecfGe81VMJ3iko5++/KfD51om
fNtLSd50nS1omUyj/Y=.ed25519

Social Consensus

Built-in governance

There must be a way for the users to determine the behavior of the network

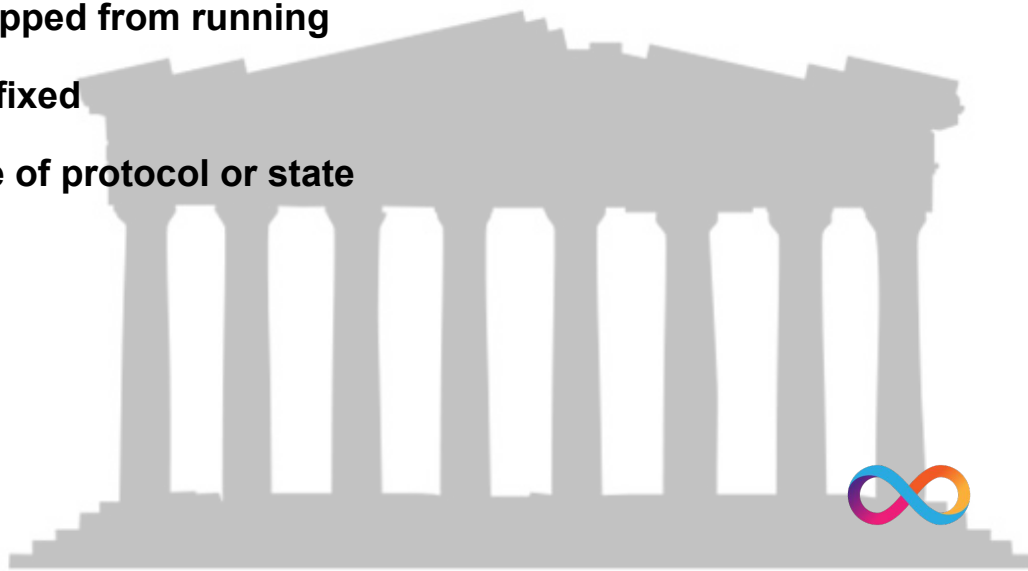
Client updates must be frequent and contention free

Updates must be reversible

Undesirable programs must be able to be stopped from running

Malfunctioning programs must be able to be fixed

Network forks are not an acceptable outcome of protocol or state changes



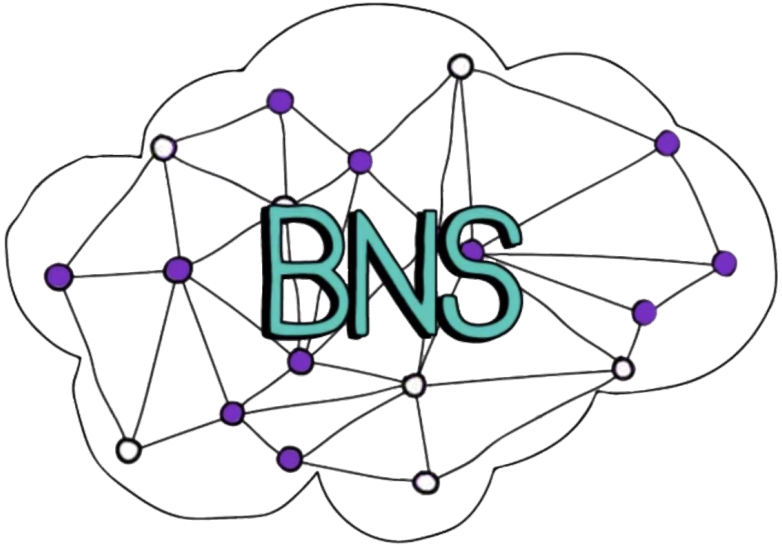
The Blockchain Nervous System: Proposals and proposers

Proposals may:

- **Upgrade the protocol**
- **Freeze undesirable programs**
- **Fix broken programs (unfreeze funds)**

Proposers might be:

- **Protocol developers**
- **Concerned citizens**
- **Businesses using the platform**
- **Machine actors identifying optimisations potentially managing sharding**



The Blockchain Nervous System: Voting and execution

Participants must place a security deposit with a long unbonding period

A fee or bond must be paid along with the proposal

Opaque Liquid Democracy structure

If the proposal passes it is sent to the BNS “SuperUser” module

The SuperUser module, with unique permissions, executes the proposal