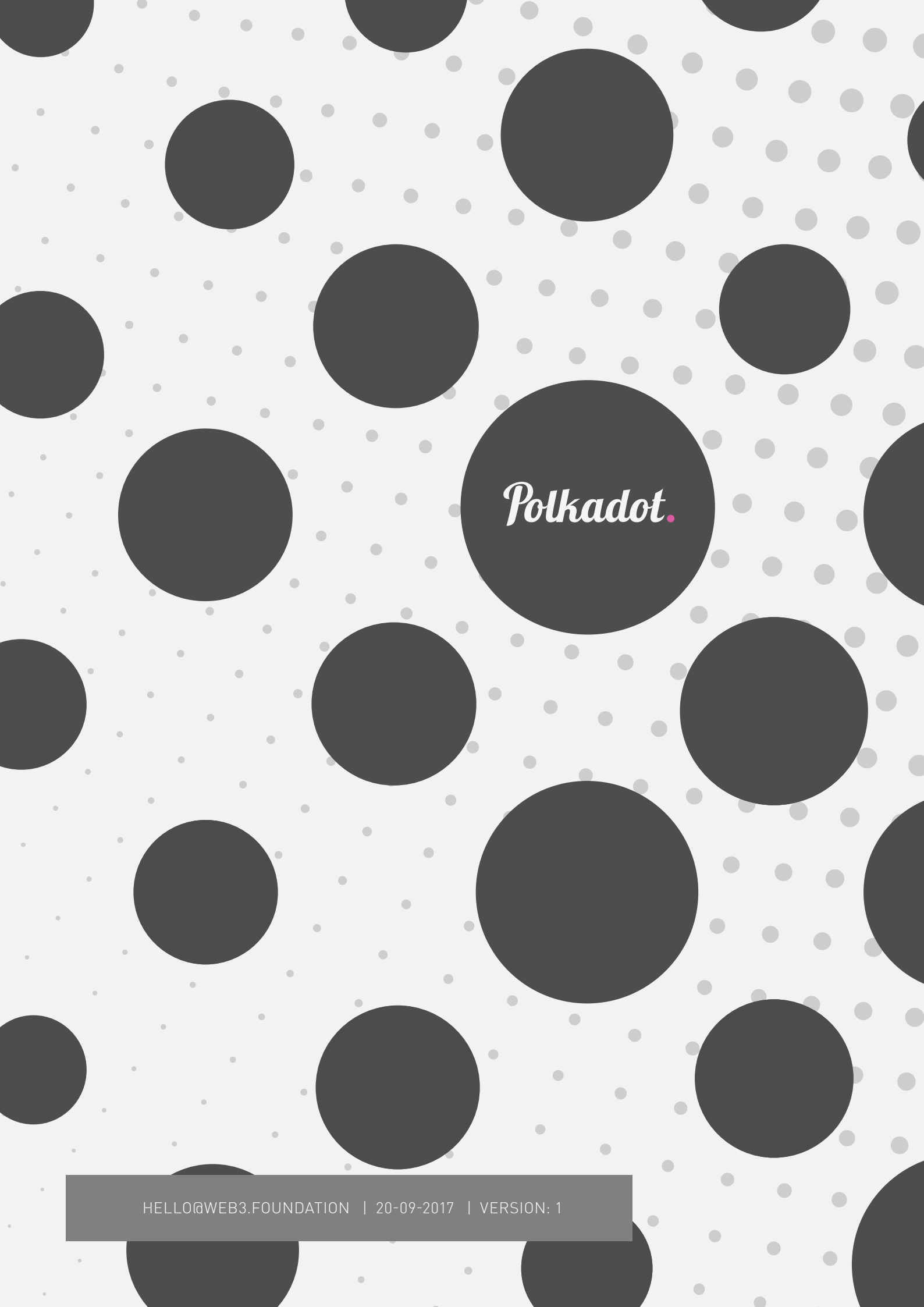


HELLO@WEB3.FOUNDATION | 20-09-2017 | VERSION: 1

Introducing

Table of Contents

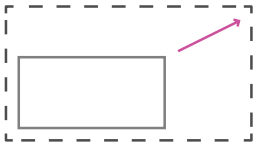
Addressing existing technology stacks

Blockchains have demonstrated great promise of utility over several fields including “Internet of Things” (IoT), finance, governance, identity management, web decentralisation and asset-tracking.

We have seen a number of blockchain and crypto projects reach significant milestones. Some are highly functional and open such as Ethereum while others provide strong privacy like Zcash. Others are designed to fulfill the permissioning requirements of enterprise and operate in private.

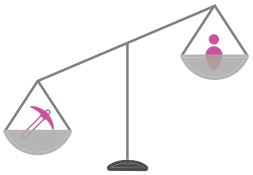
However, despite the technological promise, we have yet to see significant real-world deployment of present technology.

We have identified five key points of failure in current blockchain technology stacks.



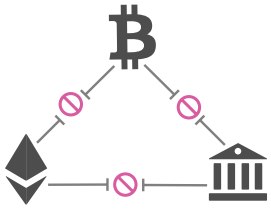
1 Scalability

Existing blockchain technology doesn't have the capacity to run the amount of transactions necessary to fulfill the promise of a decentralized world.



2 Governance

Existing blockchain governance is focused on proof of work vs proof of stake, incorrectly rewarding the few at the expense of the many.



3 Isolability

Blockchain networks exist in isolation with no communication or interoperability between them. Bitcoin cannot communicate with Ethereum which cannot communicate with private chains.

4 Developability

DApp creation is limited by the lack of integration opportunity, which exists because there is neither scalability nor interoperability in the ecosystem.

5 Applicability

Because of the lack of scalability, interoperability, and developability, end consumer use cases are not realized. Blockchain has not yet bridged the gap from core technology to actual applications, and at this point, remains theoretical rather than practical.

Polkadot is a network that connects blockchains.

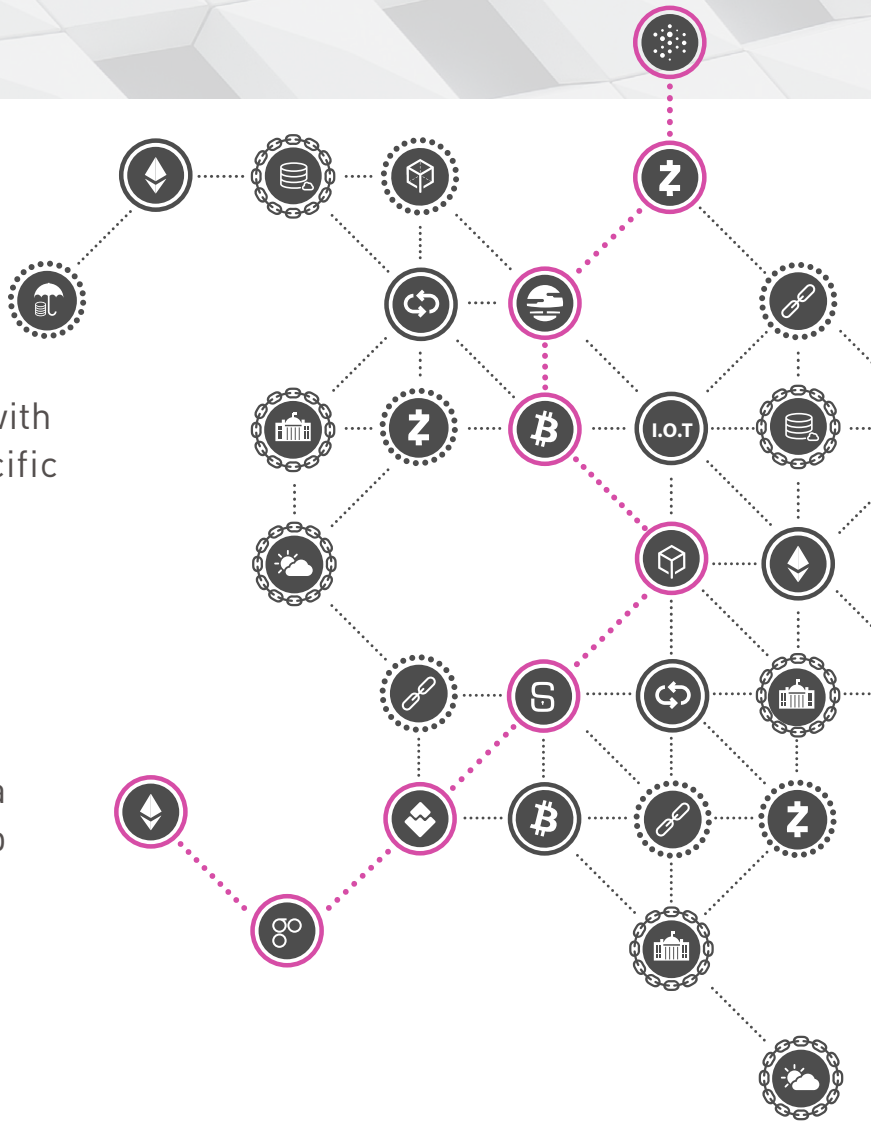
Polkadot allows new designs of blockchains to communicate and pool their security while still allowing them to have entirely arbitrary state-transition functions.

This opens to the door to a network of blockchains, where private and consortium chains can be firewalled from open and public chains like Ethereum without losing the ability to communicate with them on their own terms, not unlike the intranet/internet synergy we see today.

At a high level, here are the problems we are attempting to solve:

1. **Interoperability**
2. **Scalability**
3. **Shared Security**

Interoperability



In the future, we see a world filled with diverse blockchains all serving specific and unique purposes. Currently, these blockchain networks exist in isolation with no communication or interoperability between them.

This is an existential problem that needs to be addressed in order for a truly trustless ecosystem to develop and thrive.

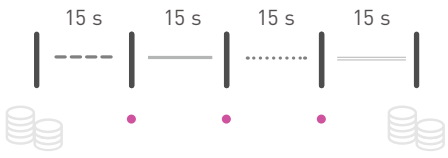
Polkadot is designed to enable applications and smart contracts on one blockchain to seamlessly transact with data and assets on other chains.

Scalability

Currently transactions are processed one-by-one on network nodes, creating a bottleneck as more transactions try to make their way through the network.

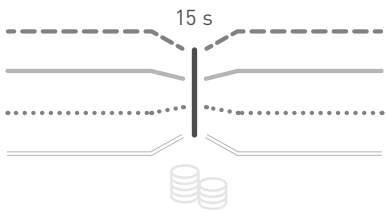
Polkadot gives the ability to run several parachains*, each processing multiple transactions in parallel, which allows networks to obtain infinite scalability.

Current Method:
Single Transactions



Because transactions have to be processed one-by-one by each node, there is a limit to network scalability.

Polkadot Method:
Multiple Parallelised Transactions



Our tests indicate a single chain can process up to around 1000 tx/s. By creating multiple parachains, we can multiply this so the Polkadot Network can securely process hundreds of times more.

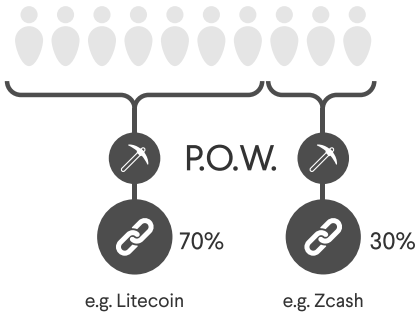
*Parachains are the name given to the parallelised chains that participate in the Polkadot network.

Shared security

Chains naturally compete with each other over security resources. They then squander it.

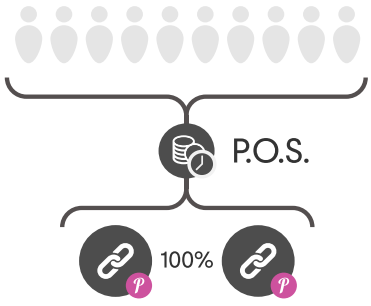
With Polkadot, security is pooled within the network, which means that individual chains can leverage collective security without having to start from scratch to gain traction and trust.

Traditional isolated security



VS

Polkadot shared security

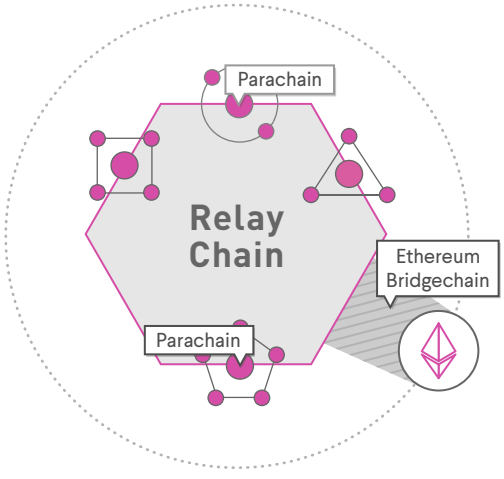


The Breakdown

Polkadot is a heterogeneous multi-chain technology.

Polkadot consists of many parachains with potentially differing characteristics which can make it easier to achieve anonymity or formal verification. Transactions can be spread out across the chains, allowing many more to be processed in the same period of time.

Polkadot ensures that each of these blockchains remains secure and that any dealings between them are faithfully executed. Specialised parachains called bridges can be created to link independent chains.

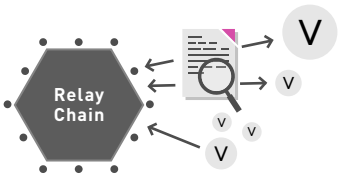


- **Relay chain**
  Coordinates consensus and transaction delivery between chains

- **Parachains**
  Constituent blockchains which gather and process transactions

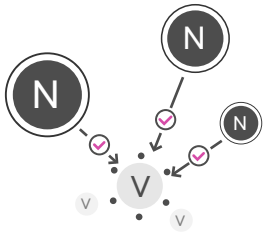
- **Bridges**
  Link to blockchains with their own consensus such as Ethereum

Polkadot Network Participant Roles



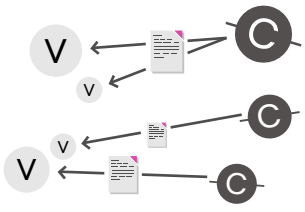
Validators

Secure the relay chain by staking DOTs, validating proofs from collators and participating in consensus with other validators.



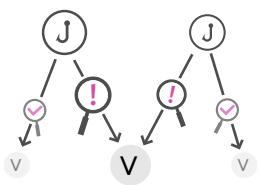
Nominators

Secure the relay chain by selecting good validators and staking DOTs.



Collators

Maintain parachains by collecting parachain transactions from users and producing state transition proofs for validators. They also monitor the network and prove bad behaviour to validators.



Fishermen

Final security frontier, they monitor the network and prove bad behaviour to validators.

Polkadot Pick 'n' Mix

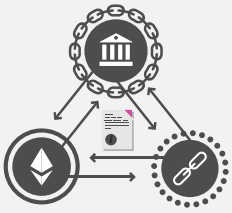
A Core Building Block

We envision a Web where our identity and our data is our own - safely secured from any central authority. It is our mission to bring a completely decentralized world from theory into reality. We call this next iteration Web3.

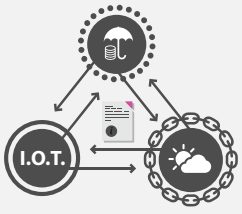
Polkadot is built to connect private consortium chains, public permissionless networks, oracles and future technological developments yet to be created in the Web3 ecosystem. It enables an internet where independent blockchains can exchange information and trust-free transactions via the Polkadot relay chain, with the key tenets of scalability, governance and interoperability.

By connecting these dots, we allow for the development of a truly decentralised internet, serving as a foundational building block for fulfilling the true promise of blockchain technology: the creation and mainstream adoption of an ecosystem of Dapps and services that will distribute power and equity for the common good.

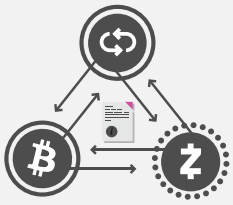
What will you create with Polkadot?



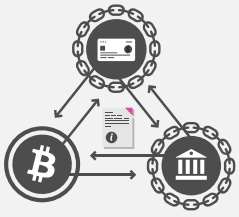
Weather oracle confirms a hurricane, IOT oracles confirm damage. Private insurance chain issues a token to payout for damages.



Blockchain project requires crowdsale contributors on Ethereum to be verified by a private bank before accepting ETH.



Decentralised exchange parachain allows users to deposit BTC using Zero knowledge proofs using a Zcash parachain.



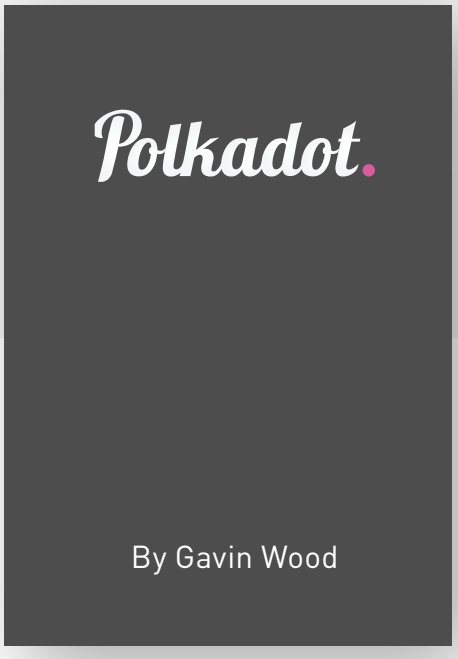
Payment processor private chain requires users to be verified with private bank chain to make purchases in BTC.

These are examples of a few use cases - there are infinite opportunities

Technical Details

WHITE PAPER

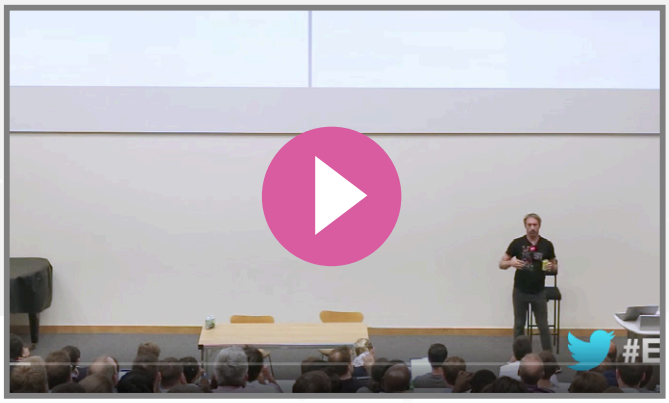
For a more in depth review on the technology behind Polkadot, take a look at our White Paper.



link:
polkadot.io/whitepaper

INTRODUCTION TO POLKADOT

Web3 Foundation Founder, Dr. Gavin Wood, speaks about the concept of Web3 and presents a high level look at how Polkadot works.



link:
https://www.youtube.com/watch?v=llghiCmHz0U

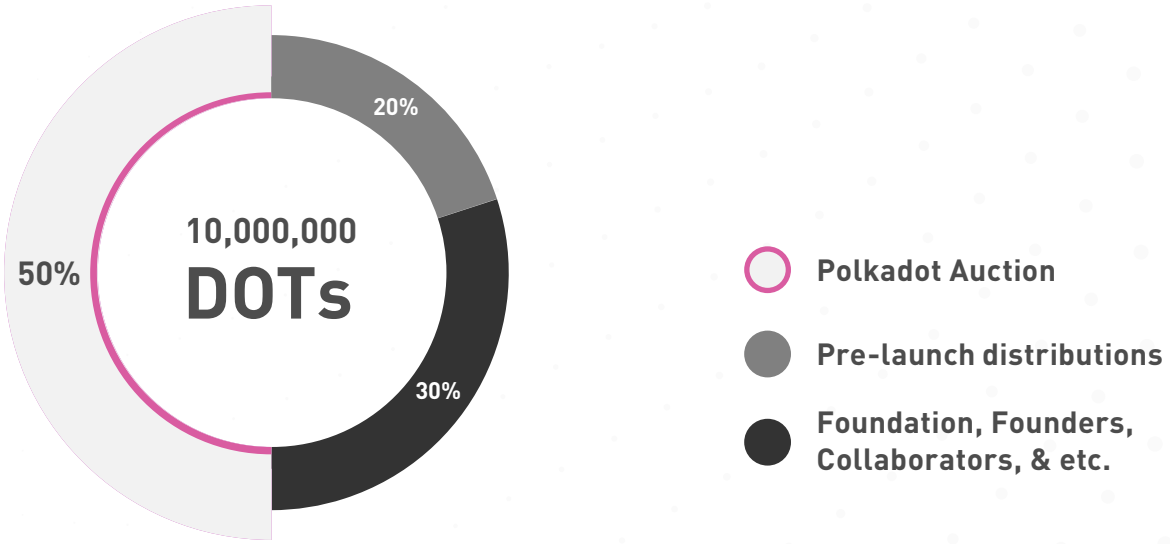
DOTs will be released in the Genesis block - estimated to happen in Q3 2019.

Technicals

The sale is a Spend-All Second Price Dutch Auction. In the auction, 5 million out of the total 10 million DOT tokens allocated at Genesis time will be sold. As an auction, by the time it finishes, it will find a "price" in order that all 5 million DOTs are happily sold.

The second-price Dutch auction model means that the provisional price at which tokens are offered starts high and lowers throughout the auction period in a predefined schedule. The auction closes once the orders received at the current provisional price are enough to purchase the entire 5 million DOTs.

Unlike normal second-price Dutch auctions, you don't bid on a number of DOT tokens given a current provisional price (which will never increase, only decrease), but rather you bid on an amount to spend, and thus will receive more DOT tokens as the auction continues and the price lowers. Everyone who participates receives the same buy-in price, which is the price that the auction ends on.



The Dot

The DOT token serves 3 distinct purposes: governance over the network, operation and bonding & payment.

Governance

Polkadot token holders have complete control over the protocol. All privileges, which on other platforms are exclusive to miners, will be given to the relay chain participants (DOT holders), including managing exceptional events such as protocol upgrades and fixes.

Operation

Game theory incentivizes token holders to behave in honest ways. Good actors are rewarded by this mechanism whilst bad actors will lose their stake in the network. This ensures the network stays secure.

Bonding & Payment

New parachains are added by bonding tokens. Outdated or non-useful parachains are removed by removing bonded tokens. This is a form of Proof of Stake.

For further information on DOTs, please read our FAQ.

Roadmap

Polkadot's Genesis block will launch in Q3 2019. Here's how we plan to get there:

Finalisation mechanism
Optimistic BFT Proof of Authority consensus mechanism.
The mechanism allows the proof of misbehaviour for the dismissal of malicious validators.

Parallelised decentralised candidate selection mechanism
This is allowing multiple independent items to be agreed upon under a single series based upon subjective reception of the partial set of validator statements. Used as an input to the finalization mechanism.

Proof of Stake chain
Extending the consensus mechanism into Proof of Stake territory; this module includes staking tokens, managing entry and exit from the validator pool, a market mechanism for determining.

Networking subsystem
This is the means by which a peer network is formed and maintained. First an altered devp2p, then libp2p.

Parachain implementation
This will include an integration with the Proof of Stake chain, allowing the parachain to gain consensus without its own internal consensus mechanism. More than likely this will include a WebAssembly-based contract execution architecture.

Transaction processing subsystem
An evolution of the parachain and relay-chain, this will allow for transactions to be sent, received and propagated. It includes the designs of transaction queuing and optimised transaction routing on the network layer.

Transaction-routing subsystem
This introduces more specifics into the relay-chains' behaviour. Management of the ingress/egress queues and network protocol with means of directed transaction propagation, ensuring independent parachain collators are not overly exposed to transactions that are not of interest.

Relay chain
This is the final stage of the relay-chain, allowing the dynamic addition, removal and emergency pausing of parachains, the reporting of bad behaviour and includes implementation of the 'fisherman' functionality.

Independent collators
This is the delivery of an alternative chain-specific collator functionality. It includes proof creation (for collators), parachain misbehaviour detection (for fishermen) and the validation function (for validators). It also includes any additional networking required to allow the two to discover and communicate.

Further non-core components

Friends of Polkadot

Polkadot is chain agnostic and is designed to work with all public, private and enterprise chains.

We are excited to work closely with the following partners to develop first use cases and look forward to working collaboratively with other blockchain projects seeking to adopt this technology.

WEB3 Foundation

The WEB3 Foundation

The WEB3 Foundation was created to nurture and steward technologies and applications in the fields of decentralized web software protocols, particularly those which utilize modern cryptographic methods to safeguard decentralization, to the benefit and for the stability of the WEB3 ecosystem.

The Polkadot network is a keystone of the WEB3 Foundation.

The Future of the Foundation:

The Web3 Foundation seeks to fund or otherwise assist in the development and deployment of projects aligned with it's mission:

- Innovative blockchain technologies, cryptographic messaging protocols.
- Peer-to-peer networking infrastructure (such as libp2p and devp2p)
- Crypto-economic mechanisms (such as DAC/ DAOsoftware)
- Data publication systems (such as IPFS).

More information:
web3.foundation
hello@web3.foundation

The Development Team

parity

The WEB3 Foundation has commissioned Parity Technologies to build the Polkadot protocol.

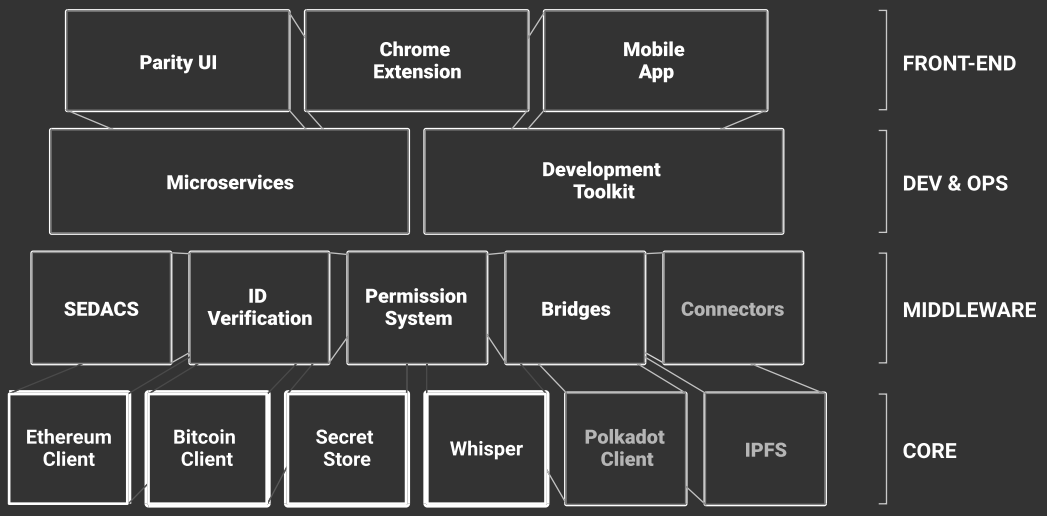
Founded by Dr. Gavin Wood, the team consists of 30 top developers who are experts in systems programming, cryptography, and distributed systems.

Parity Technologies created the most advanced Ethereum client & Wallet Application and has become the platform of choice for developers and users of decentralized applications on the public Ethereum network.

Parity Ethereum is the world's first Ethereum Virtual Machine (EVM) implementation that supports pluggable consensus engines to facilitate easy set-up of private permissioned blockchains for the enterprise. Parity is viewed as the key innovator to provide the technology for future enterprise suites relying on decentralised technology.

Parity Technology Stack

Parity Technologies stack draws directly on the power of decentralization to deliver both security and high availability. Security is realised by distributing trust amongst multiple parties with disparate interests. High availability is achieved by easily distributable storage and computation.



Further Reading

Find out more
www.polkadot.network

Join the conversation
@polkadotnetwork
#polkadot-watercooler:matrix.org

Whitepaper:
https://github.com/w3f/polkadot-white-paper/blob/master/PolkaDotPaper.pdf

Technical website by Parity Technologies LTD:
https://polkadot.io/

Dr. Gavin Wood Introduces Polkadot
https://www.youtube.com/watch?v=lIghiCmHz0U