

ASSET HIGHLIGHT



**POLKADOT** 

coinshares.com

# **POLKADOT**



## **PURPOSE**

Provide a Layer-Zero technology as an all-in-one framework for new blockchains to be created and existing blockchains to be transitioned through generalised and simple code. As a result, all chains experienced increased interoperability, shared security and forkless upgrades.

## THE SYSTEM

Scalable
Layer - Zero Technology
Interoperable
Fork-less
Easily innovative
New form of security

Source: Polkadot, CoinShares

## THE ASSET

Governance	
Not a currency	
Staking	
Bonding	

Source: Polkadot, CoinShares

## **PRICE PERFORMANCE**

2020*	88.74%
2021	240.70%

Source: DOT/USD, Compass Financial Technologies. The figures shown relate to past performance. Past performance is not a reliable indicator of future results and should not be a sole factor of consideration when selecting a product. Transaction costs, fees and expenses not included. Figures do not include any staking rewards.

## **GENERAL INFO**

Creators	Dr. Gavin Wood, Robert Habermeier, Peter Czaban
Launch	May 26th 2020
Consensus	Nominated Proof of Stake (NPoS)
Asset	DOT
Max Supply	N/A
Smallest Unit	1 Lamport = 0.000000001 DOT
Pre-Mine	42% foundations (grant pools, testnet rewards), 33% insiders (VCs, team, company), 25% public
Core Contributors	Web 3 Foundation and Parity Technologies
Language	Rust, C++ and Golang

Source: Messari at May 9 2021, Polkadot, CoinShares

## **QUICK STATS**

Market Cap	\$19.6bn
Current Issuance	1.16bn
Circulating Liquid Supply	378m (32.5%)
1 year active supply	25.6%
Annual inflation	7.88%
Mean Transaction Value (USD/day)	3653
Average new addresses (No./day)	2490
Average active addresses (No./day)	25.6k

Source: Polkadot Subscan as at 4 Feb 2022, CoinMetrics as at Feb 3 2022, YieldScan as at Feb 4 2022, Messari as at 4 Feb 2022

### **EXECUTIVE SUMMARY**

This report simplifies and clarifies what Polkadot is and what it does; the problem Polkadot tries to solve and its development since launch; its strengths and weaknesses, and opportunities and threats. As well as the people behind the protocol and the core components and network participants within the protocol.

The whole crypto ecosystem is ever-changing and dynamic, yet a consistent and growing theme over the last couple of years is interoperability and scalability. Recently, it has really come to the forefront of development and hype as to which protocol will capture the most value and usage.

These protocols are Layer-Zero which means that blockchains such as Polkadot provide a toolkit for teams and developers to create their own blockchain effortlessly on top of one network. Therefore, increasing interoperability and scalability, as well as security, in Polkadot's case.

## Layer O provides the foundation for other Layers

	Layer 0	Layer 1	Layer 2
Polkadot	N/A	Moonbeam	Injective Protocol
Cosmos	N/A	Binance Smart Chain	Alpaca Finance
Avalanche	N/A	Ethereum Virtual Machine	Pangolin
Bitcoin	Interlay, Polkadot's Bridge	N/A	Stacks
Ethereum	Gravity, Cosmos Bridge	N/A	Arbitrum

Source: CoinShares

Disclaimer: Examples are not exhaustive

## **MOTIVATION AND SOLUTION**

Currently, crypto has isolated legal systems (smart contracts), rules (blockchains) and incentives (tokens). This misalignment creates borders where borders don't need to be, thereby, increasing inefficiencies and costs for the end-user. To solve this, Polkadot was simply coded - more flexible, simple and innovative than Layer-One's. In fact, it's Layer-Zero. Layer-Zero protocols underlie, support and form the foundation of full Layer-One blockchains on top of one network.

Dr. Gavin Wood, Co-Founder of Polkadot, purposefully coded Polkadot without a use case. Unlike Ethereum, it doesn't support smart contracts. Instead, Polkadot provides a toolkit for developers to customise their blockchain to their preferences for different features such as privacy, security, speed, scalability and governance. As a result, the abstraction and generalisation of the code increased the number of blockchains on top of one network and has enhanced interoperability, shared security and decentralised updating techniques.

Last, smart contracts are convoluted and writing one's own blockchain requires huge amounts of time, trial-and-error and skill. Polkadot's Substrate is a standardised framework intended to be user-friendly for developers providing options of different languages for different functionalities and applications all connected to one network. Therefore, producing different products by different teams on different chains (Parachains). As a result, increasing Polkadot's utility as a Layer-Zero, interoperable framework for developers to create and transition new blockchains onto one ecosystem.

### **PEOPLE**

Core People: Polkadot was founded by three main people.

Dr. Gavin Wood was the Co-Founder and Chief Technology Officer (CTO) of Ethereum. Having coded his first Ethereum client released as "PoC-1" (the first Proof-of-Concept), he further co-designed ground-breaking concepts like Ethereum

Virtual Machine, gas, caller-pays account model, Solidity, Proof-of-Authority and PoC, Whisper, Javascript API and more. Gavin successfully received his Masters and Doctorate in Computer Science from the University of York and designed and implemented the first C++ set of tools. As well as founding Parity Technologies and Web 3 Foundation.







Second, Robert Habermeier is the CTO and core developer of Parity Technologies; Parachains Core Team Lead; and a member of GitHub since 2014, with over 9300 contributions to date, and a background in Rust language, distributed systems and computer security. As well as winning a Thiel Fellowship.

Last, Peter Czaban is the CTO of the Web3 Foundation and a software engineer at Parity Technologies where he built consensus algorithms such as Aura and other smart contract-based validation mechanisms. Peter has also worked on Purse.io, one of the most legitimate and widely used Bitcoin Decentralised Applications (DApps) and obtained his Master's degree of Engineering Science at the University of Oxford, where he was also a key member of The Machine Learning Research Group.

### Core Teams: Web3 Foundation and Parity Technologies



**Alistair Stewart** Head of Research



**Jeff Burdges** Research Scientist



**Syed Hosseini** Research Scientist



Handan Kılınç Alper Research Scientist



Alfonso Bolivar Cevallos Manzano Research Scientist

Source: Weh3 Foundation

Web 3 Foundation supports, researches, develops and funds open-sourced projects and decentralised protocols where transactions are secure and users 'own their data, identity and destiny' - all key components of Web 3.1 Currently, other than Polakdot, Web3 Foundation supports two main projects directly affecting the Polkadot blockchain: Kusama and Cross-Chain Message Passing (XCMP).

## Polkadot's cousin protocol

Kusama is an independent, stand-alone network that was released as the early version of Polkadot with the same code. Both blockchains are based on Nominated Proof-of-Stake and are interoperable and fork-less. However, both have different use cases. Kusama is the early stage start-up network, pre-production environment for Polkadot. It has lower barriers of entry, less security and stability, more flippant governance and faster iteration with the latest technology ideal for applications that don't need top-notch security and robustness or want to experiment, test and develop ideas. Kusama and Polkadot are complementary blockchains and communities but will live independently with separate governance.<sup>2</sup>



Source: CoinShares

<sup>1.</sup> https://web3.foundation/about/

<sup>2.</sup>https://wiki.polkadot.network/docs/learn-kusama-vs-polkadot

### Polkadot's Messaging System

XCMP is for the transaction and exchange of value and data between Polkadot's Parachains (blockchains on the network). However, due to bad actors, the transfer of value and data can be attacked, disrupted or corrupted. In the face of these issues, the Byzantine General's problem has led to several consensus algorithms to reach consensus despite these occurrences, or components of the system failing. Theoretically, in a state of war, General's (bad actors) can send false or broken messages (invalid blocks) to their counterparts (nodes). This is in relation to attacking another army (exploiting the blockchain) or defending their position for a zero-sum outcome (to break down the network). Polkadot overcomes these problems via its consensus mechanism because of its ability to be: 1) trustless as XCMP is under the same validator set as the rest of the Polkadot network so there is no need to worry about if the information contained is incorrect; 2) consistent because the protocol guarantees the messages sent were the same received despite any chain reorganisations; 3) available at all times as messages can be reconstructed if needed from the communication and conformation between the Parachain and Relaychain validators; 4) in the right order due to the input/output validation process, and 5) quick due to Polkadot's transaction speed.



Parity is different to Web3 Foundation. With over a team of 80 based in nine different countries, Parity's most beneficial project for Polkadot is <u>Substrate</u>. Substrate provides the infrastructure necessary to build custom blockchains and manipulate certain characteristics and features of a developer's customised blockchain. Teams can build their blockchain in any language that runs on WebAssembly (a platform enabling any set of instructions in different languages to be run across any machine), for example, Rust, C/C++, C#, Go and more. As well as providing all the needed network monitoring, reporting and analytical information.

### **DEVELOPMENT**

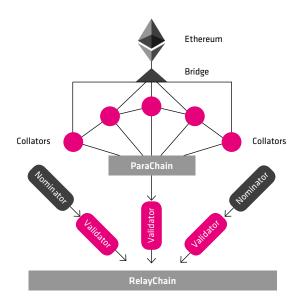
Kusama was founded in 2019 by Dr. Gavin Wood and is the pre-fix to Polkadot. As mentioned, Kusama is an independent, stand-alone network that was released as the early version of Polkadot with the same code. Both blockchains are based on NPoS, and are interoperable and fork-less but with different use cases.

2021 saw a successful year in the eyes of the developers with 16 Parachains running with around 31% of the total supply (3 million KSM (native Kusama token)) locked. As well as Polkadot auctioning five Parachain slots (for blockchains to 'bond' to the network) and, as a result, locking up approximately 106m DOT or 9% of total supply whilst increasing (x3) the number of Nominators to 22,000 and maximising the number of active Validators. Therefore, drastically improving the security and interoperability of both networks.

At the moment, both blockchains are separate from each other, however, there are plans to build decentralised bridges to link Kusama with Polkadot and Polkadot with Ethereum. This should increase Polkadot's interconnectivity and interoperability much further within the blockchain ecosystem and advance further to their goal of providing a full-stack framework as a Layer-Zero ecosystem. As well as developing their efforts to reduce costs and latency associated with XMCP to reach their goal of 1000 TPS per Parachain. This involves optimising the speed of messages (proof of transaction) to the Validators from the Collators.

## **CORE COMPONENTS**

An overview of the core components of Polkadot:

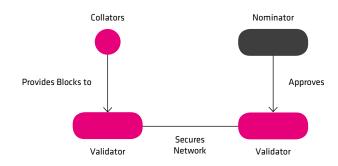


	Relaychain	Parachain	Bridge
Role	Communicates with the whole system. Limited functionality as smart contracts are not supported - only used for security, on-chain governance and Parachain auctions. Other less pertinent requirements are delegated to the parachains.	Parachains support smart contracts and are application-specific Layer- One blokchains, validated by Relaychain validators. They are connected to the Relaychain by leasing a Parachain slot.	Allows data to transfer between Polkadot's network and external networks such as Ethereum.
Importance	Central chain of the Polkadot network. If the Relaychain is breached and reverted, so does every other Parachain on the network.	Central to the Relaychains shared security and Polkadot's interoperability and scalability. Parachains are more functional than Relaychains as they are easily adaptable, customisable and have the benefits of no gas fees.	Increases interoperability and scalability of Polkadot's network as it is classed as it's own Parachain.
Security	All network participants' economic incentives focus on securing the Relaychain through Polkadot's shared security by leasing Parachain slots and stake Validators with DOT to secure the network.	Secured by other Parachains due to Polkadot's shared security. One Parachains is secured by all the other Parachains total stake.	Secured by Relay Chain
Other	Parachains auction and lease slots ('bond' DOT tokens) to become part of the network	Communicate with other Parachains using XCMP and maintained by Collators	Maintained by Collators but also can be a standalone Parachain with its own upgradable, customisable and interoperable protocols, rules and governance.

Source: Polkadot, CoinShares

## **NETWORK PARTICIPANTS**

Network Participants in the Polkadot Ecosystem:



	Validators	Nominators	Collators
Role	Mostly responsible for the securitisation of the network by 'staking' DOT	Secure Relaychain by approving good Validators	Collect and maintain all the information regarding transactions on the Parachain
Process	Receive messages from Nominators, Collators, Fishermen then check to see if the information contained in the block is valid	Nominators 'bond' their stake to particular Validators to help them become active validators (a current maximum of 297)	Produce proofs of a new block of a transaction with information, value and data inside, to be submitted to the Validator to be added to the Relaychain. As well as Send and receive messages using XCMP across Relaychain and between Parachains.
Reward	Each Validator takes a certain percentage of the inflation from the Relaychain and transaction fees. As well as tips which are voluntary	The amount 'bonded' is proportionate to rewards received, although, the work is much less than Validators, hence, the reward is fewer. But only distributed by the Validator to the top 256 Nominators for that specific Validator	Depending on the Parachain, Collators can be paid through transaction fees or the increase in value of Parachain token
Other	Two types of validators: Relay Chain Validators validate and add blocks to the Relay Chain. Parachain Validators validate blocks from Collators	In order to be paid a Nominator needs to be active - ie. nominate enough Validators (activity is key for securitisation of the network) that get elected (to validate blocks) and are not oversubscribed (less than 256 Nominators), as well as having enough DOT staked	Collators are key to Polkadot's XCMP to send messages to the Validator quickly, securely, consistently, availably and trustlessly.

Source: Polkadot, CoinShares



## DOT, THE TOKEN

### **Main Features**

Governance	Staking	Bonding
Token holders have complete authority over network	Staking sits at the core of Polkadot's consensuses mechanism, Nominated Proof-of-Stake, and, therefore, the security of the blockchain	Required for Nominators appoint Validators
More DOT staked equates to more influence over decisions	Locking tokens ('bonding') as collateral to participate in block production to reap a return	Freezing tokens in exchange for other benefits - EG Parachains lease a slot to the Relaychain during their 'bonding period' (amount of time DOT is locked)
Polkadot governance only applies to Relaychain participants	Good actors will be rewarded - members who provide blocks and validate and monitor the network	Used in the on-governance process to create proposals, second them and vote; make a treasury proposal and participate in programs
Conducted completely on-chain	Bad actors will have their stake slashed (removed to the treasury) depending on the seriousness of the attack	
	Only allowed to stake if you are a nominator or validator. Collators and Fishermen are not directly a part of the Relaychain (see "An overview of the components and network participants of Polkadot").	
	The ideal staking rate is between 50%-75% of all DOT supply depending on the number of Parachains	

Source: Polkadot, CoinShares

## **STRENGTHS**

Polkadot doubles down on its shared security. This occurs by all teams, developers and investors all using the same token (DOT) to 'bond' and 'stake' their Parachain (blockchain on top of Polkadot) to the Relaychain (main chain) in order to participate in the network and to receive rewards from securing (validating) the main chain. Moonbeam, Acala Network and Clover Finance, for example, will all have to use DOT to 'bond' their new Parachains onto Polkadot's main chain (Relaychain) and to 'stake' as a validator for security, along with other perks such as governance rights. Therefore, pooling all this capital together in the form of DOT behind the network.

Once attached to the network and drastically increasing the capital pool, this not only increases the security for your own Parachain, but every other Parachain as well, and, further, every other Parachain enhances the security of your own Parachain. As a result, the more chains that join the network, the more everyone's security increases because the capital pool from 'staking' and 'bonding' is larger which makes it harder for a malicious actor to attack.

Secondly, forkless upgrades are also a large strength of Polkadot. The simple, decentralised process occurs by a proposal being added to the queue, which is then seconded by token holders, and, then, voted on in a referendum. If it passes all of those steps then the amendment is added on-chain and is automatically updated by all the Validators (nodes) in a rolling time period. There is no human intervention or centralisation, and if the vote doesn't pass then nothing happens.

This is great for builders of the blockchains and end-users of the network because it means Polkadot and its Parachains can seamlessly upgrade to the best technology every time as seen from previously updating without hard-forking to Proof-of-Concept 2 two months after Proof-of-Concept 1. Contributors and developers around the world can easily adapt to the challenges they face, and, as a result, reduce the number of teams forking off in different directions and, instead, collate the number of developers working on the advancement of their own protocol.

Forking takes a huge amount of energy, money and consensus but this still happens because the incentives and rules are very hard to change and not agreed upon.

Polkadot reduces these problems and so the innovation capabilities provided by this process makes Polkadot and its Parachains future proof.

Last, interoperability is essential and core to the Layer-Zero nature of Polkadot. The increased number of Parachains attached to the main chain, as well as 'bridges' facilitate communication and the transfer of value, tokens and data within and between the Polkadot network and different Layer-Ones such as Ethereum, Bitcoin or Solana. This scalability for Parachains acts as a positive feedback loop and will only entice further adoption of the network.

### **WEAKNESSES**

First, Polkadot has previously experienced hacks of their multi-sig wallet. Around \$120m was frozen, in two bouts, over a course of 4 months. However, it is important to note that this also happened to some large wallet holders on Ethereum as well. To stop this black swan event from occurring again the core team at Parity Technologies have done 4 main things: 1) revisited every line of code that related to wallets; 2) added one more line of defence to ensure this couldn't happen again; 3) they've redesigned the UI to make it more inviting for developers to access their open-source code. As the more eyes that are on the code, the more developments that should occur and, therefore, reducing the chance of hacks happening again; 4) the team at Parity have also submitted some amendments to the Solidity team to change the solidity language, as they felt some code was also subject to some blame!

There's a large difference between hacking Polkadot's main chain rather than hacking Polkadot's multi-sig wallet. However, theoretically, if Polkadot's main chain were to be breached - it would revert and cause all other Parachains to revert, as well. Therefore, breaking down the network. Hence, every Parachain doubles down on the shared security aspect to prevent this from occurring.

Second, Collators (network participants who create the blocks) can send unavailable messages to the Parachain validators. This activity slows down the network because this increases the number of validators needed to validate these untrustworthy blocks, and, therefore, the network consumes more resources. Unfortunately, as mentioned in the white paper, there is no way to measure the reliability and validity of such reports which attests to the fact that there is no solution, or the solution has not been found yet.

Last, the Council comprises 13 members which is clearly a threat to its decentralisation. The Council is instructed to control the treasury, propose or cancel the referendum process (the last part of the forkless updating process) and elect the technical committee who can veto proposals.

For an update to be rejected, only one Council member out of 13 can veto the proposal. This could potentially decrease the value of DOT as stakeholders ('bonders' and 'stakers') also have governance rights from the proportion of their amount of DOT held. But, if one actor can veto a heavily favoured proposal, then the value of their governance rights, and, therefore, DOT decreases hugely.

However, there are centralisation constraints in place such as the fact that elections are held every two weeks for DOT holders to elect their preferred council member for the upcoming available seat. There are two negatives to this: 1) the frequency could lower voter turnout and reduce the representation of the preferred actors on the Council; 2) within the low turnout, bad actors have a higher chance of being elected and disrupting the network.

Conversely, this negative is reduced by introducing the 'loss-weighted' function - the runners-up of the previous election are benefited in the next election. Therefore, in theory, consistently high-value members are more likely to be elected the next time around.

## **OPPORTUNITIES**

We are currently at an inflection point for interoperability of the crypto market. 2020 and 2021 saw these ideas catch on with some upside in adoption. We are currently getting deeper into a phase where we are moving away from an independent crypto ecosystem to a new dimension where chains can communicate, plug into, exchange and leverage data from one another. It's the same as transforming from the isolated nature of nationalism to an interconnected, globalised world. More data and value is created at faster speeds with much more innovative and competitive developments that are beneficial to the end-user. A prime example is Polkadot developers being able to use Chainlink by connecting smart contracts and using all their data whilst accessing Polkadot's speed as well.

Depending on what users prefer and developers can optimise for adoption - scalability, security, decentralisation and more - will stand the test of time. Polkadot is already in a unique place where its adoption is higher than its competitors, and, therefore, improves its interoperability, scalability and security as a whole.

## **THREATS**

## Comparison between the major Layer 0's

Layer-Zero Competitors	Cosmos	Avalanche	Polkadot
Scalability	- 4000 TPS - unlimited blockchains	- 4500TPS - unlimited blockchains	goal is 1000TPS per blockchain - limit of 100 blockchains
Decentralization	<ul><li>✓ ✓ ✓</li><li>- Unlimited number of Validators</li></ul>	<ul><li>✓ ✓ ✓</li><li>- Unlimited number of Validators</li></ul>	Short term goal of a maximum of 1000 validators - Increase with demand
Shared Security	- Optional - Every chain has own security with own validator	Optional - Every chain has atleast one validator connected to main chain	- Mandatory - Every chain secured by one set of validators using one token (DOT) - However main chain is the single point of failure
Adoption	<b>♥ ♥</b> - 297 Dapps	- Founded in 2018 and ICO'd in 2020, approximately 2-3 years after Cosmos and Polkadot	<ul><li>Section 2. Section 2. Se</li></ul>
Interoperability	Bridge with external chains Communicate between own chain	Bridge with external chains Communicate between own chain	- Bridge with external chains - Communicate between own chain

Source: CoinShares

The threat to Polkadot is its Layer-Zero competition involving Cosmos and Avalanche. Overall, Polkadot is more consistent and well-rounded and emphasises shared security which is partly reflected in its adoption. However, compared to its competitors it is arguably less scalable or decentralised.

## MARKET PARTICIPANTS

The demand for crypto and its subsequent price action has mostly stemmed from the increase in investor risk tolerance, search for yield and speculation. As well as increased knowledge and curiosity, Crypto's value-locked and potential for this industry as a whole. There are approximately <u>226</u> markets to buy 'spot' DOT and <u>33</u> accessible derivative markets of DOT 'perpetuals' and 'futures'.

Polkadot has yet to find its market dominance, especially as the interoperability landscape is fiercely competitive with Cosmos and Avalanche increasing the size of the pie. However, as Hedge Funds, Asset Managers, High Net Worth Individuals and Institutions diversify and allocate into this area, deepen the capital markets, increase liquidity and reduce volatility. Brokers, market makers and exchanges will naturally increase their suite of products and services, most likely further transforming the whole crypto space and Polkadot into a time-served, mature asset class. As a result, reflecting Polkadot's success of being a fully-stacked framework to create and transition more blockchains onto the Polkadot ecosystem, and, therefore, enhancing interoperability, security and fork-lessness.

### **Disclosure**

The information contained in this document is for general information only. Nothing in this document should be interpreted as constituting an offer of (or any solicitation in connection with) any investment products or services by any member of the CoinShares Group where it may be illegal to do so. Access to any investment products or services of the CoinShares Group is in all cases subject to the applicable laws and regulations relating thereto.

This document is directed at professional and institutional investors. Investments may go up or down in value and you may lose some or all of the amount invested. Past performance is not necessarily a guide to future performance. This document contains historical data. Historical performance is not an indication of future performance and investments may go up and down in value. You cannot invest directly in an index. Fees and expenses have not been included.

Although produced with reasonable care and skill, no representation should be taken as having been given that this document is an exhaustive analysis of all of the considerations which its subject-matter may give rise to. This document fairly represents the opinions and sentiments of CoinShares, as at the date of its issuance but it should be noted that such opinions and sentiments may be revised from time to time, for example in light of experience and further developments, and this document may not necessarily be updated to reflect the same.

The information presented in this document has been developed internally and / or obtained from sources believed to be reliable; however, CoinShares does not guarantee the accuracy, adequacy or completeness of such information. Predictions, opinions and other information contained in this document are subject to change continually and without notice of any kind and may no longer be true after the date indicated. Third party data providers make no warranties or representation of any kind in relation to the use of any of their data in this document. CoinShares does not accept any liability whatsoever for any direct, indirect or consequential loss arising from any use of this document or its contents.

Any forward-looking statements speak only as of the date they are made, and CoinShares assumes no duty to, and does not undertake, to update forward-looking statements. Forward-looking statements are subject to numerous assumptions, risks and uncertainties, which change over time. Nothing within this document constitutes (or should be construed as being) investment, legal, tax or other advice. This document should not be used as the basis for any investment decision(s) which a reader thereof may be considering. Any potential investor in digital assets, even if experienced and affluent, is strongly recommended to seek independent financial advice upon the merits of the same in the context of their own unique circumstances.

This document is directed at, and only made available to, professional clients and eligible counterparties. For UK investors: CoinShares Capital Markets (UK) Limited is an appointed representative of Strata Global Limited which is authorised and regulated by the Financial Conduct Authority (FRN 563834). The address of CoinShares Capital Markets (UK) Limited is 82 Baker Street, London, W1U 6TE. For EU investors: Napoleon AM (napoleon-am.com) is a French asset management company regulated by the Autorité des Marchés Financiers (AMF), registered under number GP-19000015 since 27/03/2019. Its office is located at 11 rue Paul Lelong, 75002 Paris, France.

The CoinShares Astronaut is a trademark and service mark of CoinShares (Holdings) Limited.

Copyright © 2022 CoinShares. All rights reserved.



ASSET HIGHLIGHT

research@coinshares.com

