Polkadot

Those of you who have been following along the lines of blockchain development are well aware about the different problems that exist within the architecture of blockchain protocols.

The two major talk of the town is scalability & extensibility. The two most prominent reasons for causing this is- canonicality & validity.

Blockchains in the past have showed a lot of promise in the fields like- Internet of things. Identity management web decentralization & asset tracking.

Despite all of these promises, the technological stack fails on the following parameters:

1) Scalability.

2) Isolability.

3) Developability.

4) Governance.

5) Applicability.

Welcome to a brand new episode of Colorful white paper. In this episode we will learn about the white paper of polkadot which was written in Novemba of 2016.
The protoca was created by Ethereum co-founder Gavin wood and developed by web3 foundation with initial implementation by parity technologies.

In this white paper we will explore the first two issues of scalability & isolability. Before we dig deeper into the white paper please note that this version of paper was written in Nov of 2016. Many of these concepts might have been revised or changed; However it is very important to understand the concepts to understand the underlying

technology.

Think of yourself as an architect who is studying the structure of an old building. The structure might have been painted new, but the foundation remains the same.

Before we start analyzing the white paper, let us take a step back to understand what is the real world problem for a Blockchain.

So, the present day problem of "low number of tx" per second stems from the root cause of - number of parties agreeing on the history of state.

Think of it like you need to perform a task which needs an agreement from "most" of the parties. This might be a good solution for many usecases but one size fits all cannot be applied.

The concept is popular in both- proof of stake like Ethereum & proof of work like Bitcoin.

Previous Work:

A novel approach proposed by tangle was arranging the blocks in a "graph" instead of linked list. Now, if you know about data structures you know that traversing through a graph is easier than linked list.

This graph would be able to define the "relevant" state transition, making it possible for multiple coherent parallel states.

However, without a hard global coherency, & interaction with other systems which by the way needs an absolute degree of knowledge over system state becomes impractical.

Another proposed approach was using sidechain to bitcoin. This could act like a trustless way for sidechain to be the custodian of main chain.
By all means, this is more of "extensibility" than scalability for the existing chain.

The paper also goes in detail - about cosmos as proposed by Jae kwon's tendermint algorithm & cosper - which is a scalability model on top of Ethereum network.

For the simplicity of this draft, we will not go in detail of these approaches. They will be discussed in draft for cosmos & ethereum respectively.

As we have been digressing the different approaches - let us quickly summarize what polkadot stands for. In the next part of the draft we will dig deeper into the underlying technology that polkadot promises.

Polkadot is a scalable heterogeneous multi-chain. This means that unlike previous blockchain implementations, which have focussed on providing a single chain of varying degrees of generality over potential applications, Polkadot itself is designed to provide no inherent application functionality at all. Rather, polkadot provides the bedrock "relay chain" upon which a large number of validatable, globally-coherent dynamic data structures may be hosted side by side.

The white papers calls these data structures "Parallelized" chains or parachains, though there is no specific need for them to be blockchain in nature.

In other words, Polkadot may be considered equivalent to a set of independent chains e.g. the set containing Ethereum, Ethereum classic, Namecoin & Bitcoin except for two very important points:

1) Pooled security.
2) Trust free interchain transactability.

Philosophy of Polkadot:

Polkadot intended to provide a rock solid foundation on which the next generation of consensus algorithm could be built.

The idea was intended for a wide spectrum of ideas like - those which are production capable to those which are just intended as a joke. Thats trying to fit in a lot of use cases.

The paper also talked about how it sees the mature chains like Ethereum & bitcoin outsourcing major computational work to VM based chains

The paper proposed to use governance structure similar to a stable political system. That might be a funny analogy, but we should take it with a pinch of salt.

There will be 2 chambers formed: One of "users" which are bonded validators and the other "technical" community, consisting of developers & ecosystem players.

The body of token holders (i.e. validators) would maintain the ultimate legitimacy & form a supermajority to augment, reparameterize, replace or dissolve this structure; something the paper claims will not have a need for.

The initial primary role defined for polkadot architecture was: Minimal, Simple, General & Robust.

Now, as we understand the philosophy of polkadot, let us headover to the next section of paper which talk about participation in polkadot network.

Participation in Polkadot...

There are 4 basic roles in the upkeep of a polkadot validator. They are: Collator, fisherman, nominator & validator. Let us spend some time understanding the role of these actors.

Validators:

Validators are on the highest charge and help seal new blockchain or network. A validator must maintain a high availability and bandwidth. The process for validation looks like: Receiving nomination to add a block, validating it and republishing the candidate block from its parachain.

The process although seems deterministic, cannot be predicted much in

advance. For obvious reasons validators cannot be expected to maintain record of all parachains. Hence, there is a third party collator about which we will talk later.

Once the sub group of parachain has been ratified, validators need to relay the block itself. This involves updating the state of transition. The validator not performing its duties might be punished. For initial, unintentional failures the rewards may be withheld. For repeated offenders a part of their reward might be burned. Malicious actors like those attempting to conspire to add invalid block might end up loosing all of their bond.

Nominators:

Nominators are like silent partners who have no major role except for providing capital placement in the validators they trust.

Collators:

Tx collators are parties who assist validators in producing valid parachain blocks. They maintain a "full node" for a particular parachain; meaning that they retain all necessary information to be able to author new blocks & execute tx. Under normal circumstances they will collate & execute tx to create an unsealed block, and provide it together with zero knowledge proof to one or more

validators presently responsible for proposing a parachain block.

Fisherman:

Fishermans are a bit different from the other two parties, i.e. they provide no direct contribution to network.

Think of fisherman like hunters who scavenge through the field for wild pigs. The farmers are benefited because their crops are safe; hunters are benefited because they are rewarded.

Similarly, the benefit of fisherman is that they get rewarded for finding malicious actors and the network is rewarded by keeping it free from corruption.

Design Overview:

In this section of the paper, we will learn about the design briefly.

1. Consensus:

On a relay chain, Polkadot achieves low level consensus over a set of mutually agreed valid blocks through a modern asynchronous Byzantine fault Tolerance algorithm inspired by Tendermint.

For Proof of Authority type network, this alone would be sufficient, however Polkadot is imagined to be also deployable as a pubic network for which honesty needs to be incentivized as in Proof of Stake based system.

2. Proof of Stake:

Validators are elected through Nominated Proof of Stake as frequent as once per day or as rare as once per quarter. A portion of stake is bonded for staking & remains bonded after duty of validate ceases. (Around 3 months.)

This long bonding ensures safeguard against any misbehaviour that might uncover later.

The offending parties are punished with respect to the damage caused by them to the network.

3. Parachain & Collators:

Each parachain gets similar security affordances to relay chain: the parachain headers are sealed within the relay chain block ensuring no reorganization, or double spending is possible. Polkadot also provides strong guarantee that parachain state transitions are valid. This happens through the set of validators being cryptographically randomly segmented into subsets.

4. Interchain Communication:

The final critical ingredient of Polkadot is interchain communication. Since parachain can have some sort of information channel between them, the paper calls Polkadot as "scalable multi chain."

These parachains donot have a fee associated to it, but is rather negotiated at the source & destination of parachain.

Parachain are resolved using a simple queuing mechanism around the Merkle tree to ensure fidelity. To prevent a parachain from spamming another parachain, it is required that destinations input queue might not be larger than

previous block. If i/p is too large, then it is considered saturated & no tx might be routed within the subsequent block until reduced back below limit.

The next section of the white paper discusses the interoperability between polkadot & ethereum and polkadot & bitcoin. For the sake of simplicity, we will not be going in detail for each of these design sections.

This could be a seperate draft series where I talk about different chains by comparing & contrasting them.

Protocol Depth:

The protocol can be broken down into three parts: consensus mechanism, parachain interface & interchain tx routing.

1. Relay chain operation:

The relay chain will be broadly similar to that of ethereum with some key differences:

a. Contracts cannot be deployed through tx; that is there will be no support for public deployment of contracts.

b. Compute resources (i.e. gas) is not accounted; because a flat-fee structure is implemented.

c. Special functionality is supported for listed contracts that allows auto execution & network msg output.

2. Staking Contract:

It allows an account to register a desire to become a bonded validator.

It has 3 subsections:

a) Stake coin liquidity.

b) Nominating.

c) Bonding confiscating / Burning.

Think of stake coin liquidity as the ratio of investment to profit. The more you invest or stake, the more handsomely you are rewarded.

For people who want to invest or stake their money or DOT tokens but also don't want to get into the hassle of becoming a validator can simply nominate, i.e. invest in some trusted validator.

Pro Tip: Be careful with whom you validate. It could not only be a loss to your money, but also to the entire network.

Lastly, if you try to act smart & fool the network or behave maliciously, you might be punished.

4. Sealing relay blocks.

Sealing involves the collection of signed statements from validators over validity, availability & canonicality of a particular relay chain block & the parachain blocks that it represents.

Think of it like the project report you submit back to your manager after you complete a task.

With the only difference being. you cannot call in sick & extend your deadline!

5. The next section of the paper talks about how the scaling can be improved. Let us quickly skim through these subsections:

a. Introducing latency.

b. Public participation.

c. Availability guarantors.

d. Collator preferences.

e. Over weight blocks.

f. Collator insurance.

Again, these are very interesting topics. but for the sake of simplicity we will avoid these sub sections.

6. Interchain transaction routing.

Interchain tx routing is one of the essential maintanence tasks of the relay-chain & its validators.

Validators are incentivized only to form consensus on a parachain block.

Let us look through the subsections of Interchain tx routing:

a) External data availability.

b) Posts routing.

c) Critique.

d) Hyper cube routing.

e) Maximizing serendipity.

Like before, I think we can skip through these subsections. Remember this was more of an idea than a practical approach...

7. Parachain validation:

A validator's main purpose is to testify that a parachain's block is valid.

The process itself is very simple - once the validator sealed the previous block they are free to begin working to provide a candidate parachain block candidate for next round of consensus.

8. Networking:

The requirements for polkadot are rather substantial. Rather than a fully uniform network, polkadot has several types of participants each with a different requirement over their peer makeup & several n/w avenues whose participants will tend to converse about particular data.

Conclusion:

In this white paper we learned how one can author a scalable, heterogeneous multichain protocol with the potential to be backwards compatible to certain pre existing blockchain networks.

The white paper gave rough outline of the architecture including the nature of participants, economic incentives & process under which they must be engaged.

Thank you for
reading colorful
white paper

Peace!