The Ardor business case in a nutshell

Existing problems in the blockchain world

1. Blockchain Bloat – every transaction ever submitted to a blockchain will stays forever in the blockchain and must be re-validated by every new node which joins the blockchain.
2. Dealing with multiple tokens in the context of a single transaction – when creating a blockchain based token, users need to transact in this token but also pay transaction fee in the main blockchain token.
3. Crypto exchanges represent a systematic risk to user funds – when converting fiat money into crypto, users typically has to use 3rd party exchange web sites which represent a single point of failure and complicates the flow of funds.

About Ardor

The Ardor technology is based on the stable and reliable NXT blockchain source code which has been running successfully as a public blockchain since November 2013. Every existing function of the NXT blockchain will be supported by Ardor.

In addition, the Ardor blockchain has a unique design composed of a single parent chain responsible for the proof of stake process and multiple child chains responsible for the operational transactions such as asset exchange, voting, messages etc.

Child chains transactions are reported to the parent chain using a new process called "bundling". The bundlers, package multiple child chain transactions into a single ChildChainBlock transaction on the parent chain. The bundlers pay the transaction fees in Ardor and receive the child transaction fees.

The first child chain of the Ardor platform is called "Ignis". Ignis will inherit some of the existing state of the existing NXT blockchain.

Unlike "side chains" and other blockchain related technologies, the Ardor parent and child chains are based on the same source code and share the same security guaranties.

Let's see how the unique Ardor blockchain design addresses the problems described above

1. Blockchain Bloat
    a. The Ardor parent chain only stores transactions which affect the balances of the forgers (proof of stake block validators). All other transactions are off loaded to the child chains.
    b. Transactions stored on child chains can be pruned i.e. removed from the blockchain after 24 hours leaving only a cryptographic proof (hash) proving their former existence.
    c. A new node joining the blockchain will only need to validate the parent chain transactions, which represent only a small proportion of the transactions and the last 24 hours transactions of each child chain, not the full transaction

history. In addition, a new node will load a snapshot of the current blockchain state (account balances, properties, aliases etc) from one of the existing nodes.

   d. Individuals or entities which need the full transaction history for their own book keeping can still store it by setting up an archival node which maintains the full transaction history based on various conditions. These entities will be able to prove that a given transaction, while no longer stored on the blockchain, was presented there in the past.
   e. We estimate that this design can reduce the number of transactions stored on the blockchain at a ratio of up to 1:100
   f. In the future, Ardor child chains may even run on their own subnet where all nodes except one are disconnected from the rest of the Ardor platform thus providing the ability to componentize the blockchain into domain specific sub-blockchains and prevent the need for every blockchain node to process all blockchain transactions.

2. Dealing with multiple tokens
   a. Users of an Ardor child chain will only deal with the child chain token both for transfer of value and fee payment.
   b. When tokens such as assets or currencies are issued on top of a child chain, users of these tokens pay transaction fees denominated in the child chain token.
   c. For certain applications, a business entity managing the child chains may choose to cover these transaction fees for their users or to not charge transaction fees at all.
   d. This business entity will serve as the transaction bundler to make sure that the child chain transactions are included in the parent chain
   e. Users of asset and currency tokens on this child chain, or users using the voting system, won't need to pay transaction fees and may not even be aware that they are using a blockchain under the hoods.
3. Crypto exchanges represent a systematic risk to user funds
   a. On top of the Ardor platform, a 3rd party business entity can issue a "pegged child chain". This business will guarantee that the child token is pegged at 1:1 ratio to a fiat currency such as EUR, USD or to another crypto asset like BTC or a certain commodity value.
   b. Users who trust the business entity which guaranty the peg, can use the child chain token as if it was the base asset, allowing trading of blockchain based tokens against the base asset without the need to exchange their tokens first into the Ardor token.
   c. While the business risk for the 3rd party peg failing on its promise still exists. The technical risk for user funds is vastly reduced by storing the account balances on blockchain.