appliedblockchain

Gartner
GLOBAL TOP 20 BLOCKCHAIN CONSULTING FIRM 2017-2020

2021 REVIEW OF NEXT GENERATION ENTERPRISE BLOCKCHAIN TECHNOLOGIES

By Applied Blockchain

appliedblockchain.com
info@appliedblockchain.com

Table of contents

Introduction

As we approach 2021, five years since the launch of the first generation of enterprise distributed ledger platforms, we review the next wave of state of the art blockchain platform technologies.

Platforms To Be Reviewed

The first generation of enterprise platforms prioritised data privacy over broad consensus and security. That is, networks were reduced into smaller “channels” with very few validators in order to provide data privacy.

A range of new DLT platforms are becoming available to enable private transactions verifiable by a large network. The platforms that we will assess are split into two categories.

Enclave Platforms

Platforms that use secure enclaves to securely process and validate transactions without revealing the details of the transaction to the party hosting the node or even the operating system that is being used to host the node.

Corda and the Conclave Platform

Microsoft Confidential Consortium

Zero Knowledge Platforms

Platforms that use zero knowledge proofs where transactions are processed locally and a proof which does not reveal details of the transaction is submitted to the blockchain for validation.

The Baseline Protocol

The Aztec Protocol

Adi Ben-Ari

Founder & CEO, Applied Blockchain

Andrew Campbell

Solution Architect, Applied Blockchain

Chapter 1: Blockchain & Data Privacy

One of the most common misconceptions that we come across almost daily is the belief that blockchain technology keeps data private.

Blockchains are designed to group-secure transaction history. This is their primary function, and it is also why they are great for recording asset (token) ownership and movement.

Blockchains do not protect access to data. The blockchain mechanics do not, in general, manage data privacy, access to data or protection of data. If anything, they increase the footprint of any data stored in a blockchain, increasing risk of a data breach.

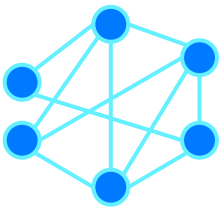
In fact, the original blockchain, Bitcoin, is completely transparent, and is a perfect example.

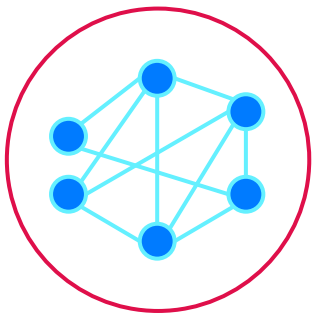
However, many blockchain applications, especially in enterprises, require some level of data privacy, such that not all participants in the network can see each other's transactions and data.

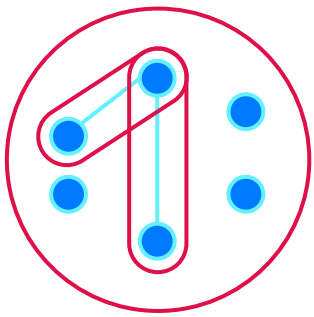
Blockchain platforms initially provided two solutions:

1. Encrypt the data. The problem with this approach is that any data or transaction that is encrypted cannot be independently validated by a node that is not able to decrypt, and therefore see the data.
2. Isolate the data and transactions. This is the pattern that most enterprise blockchains adopted. The problem with this approach is that it radically decreases the number of parties that can validate the integrity and security of a transaction, which undermines the very premise and advantage of using a blockchain in the first place.

A new generation of technologies, namely secure enclaves and zero knowledge proofs enable us to have both transactional and data privacy, as well as a broad and secure set of transaction validators.







First we had open, public networks

...then we closed them and made them private among a consortia of companies

...and isolated further, each time reducing the number of validators

Chapter 2: Enclave Platforms

Hardware secure enclaves provide an environment where code can be executed in private, with no access given to the host computer or operating system.

The foundation for these new distributed ledger platforms is Intel SGX, a range of chips that support running code and storing data in enclaves. These enclaves offer an execution and storage environment that is inaccessible to the operating system and user no matter what privileges the user has. The chip achieves this by encrypting data before storing it and only decrypting it at runtime within the CPU. SGX CPUs also offer cryptographic proof of what code was run within the enclave and signed output which can be validated later.

As we can run arbitrary code within the enclave we can securely generate keypairs within the SGX enclave, these keypairs can be verified as generated within the enclave. This enables secure SGX to SGX communication over a network via asymmetric encryption. This has enabled organisations to create blockchain architectures within the SGX environment.

Considerations

Security

There have been a number of vulnerabilities found within the SGX architecture the most recent being SGAxe which allows a party to gain access to attestation keys. Intel has responded to these vulnerabilities and is patching them through microcode updates.

Performance

The speed of execution of code in an SGX enclave is comparable with that of a regular CPU allowing for a high throughput of transactions.

Portability

Because SGX is a CPU level innovation applications built on top of it need to run on SGX enabled hardware. However cloud providers including Azure have launched SGX machines as a service.

2.1 Microsoft Confidential Consortium Framework (CCF)

Microsoft CCF is an open source framework built on top of SGX. The framework creates an encrypted ledger each instance of which is stored inside an Intel SGX enclave.

Nodes are run by authorities, each authority must host the node on a machine with access to SGX. The framework supports Raft and Practical Byzantine Fault Tolerance (PBFT) consensus mechanisms and transactions are accepted when agreed by a variable number of nodes. The ledger consists of a key value store held encrypted by each party, the integrity of which is confirmed by a merkle tree. The keystore supports both encrypted and unencrypted key/value pairs for flexibility.

SGX is used to provide attestation that all nodes are running within an SGX enclave and that all nodes are running the same code within that enclave. This gives us a smart contract environment backed by SGX with output written to an immutable ledger. Relying on SGX for private transactions enables CCF to have throughput comparable with a database with speeds of five thousand transactions per second reported by Microsoft.

Requirements	Platform Support
Verifiable Transactions	Yes, transactions verified in SGX
Private Transactions	Yes, transactions encrypted and processed in enclave
Scalable	Yes, 5000tps
Immutable Transactions	Yes, datastore backed by merkle tree
Flexible Governance	Yes, multiple consensus mechanisms available with authorities added and removed
Group Security	Yes, full copies of the ledger held by parties running nodes
Production Readiness	Being used by 1st party (Microsoft product teams) and 3rd parties today for production, HA use cases.

Additional Considerations	
Ease of Development	Very good docker containers for development and testing, smart contracts written in c++
Ease of Deployment	Very good example scripts for Azure deployment
Flexibility of Deployment	Somewhat, deployment requires SGX enabled hardware. SGX hardware is currently offered by Microsoft Azure, IBM Cloud & Alibaba cloud
Requires Crypto payment for transactions	No

2.2 Corda and the Conclave platform

Corda is an enterprise DLT platform capable of allowing multiple organizations to interact with each other.

There is no globally shared ledger in Corda, instead parties communicate with each other through channels and each party keeps a record of the facts it is aware of. Immutability of transactions is ensured by sending signatures to a notary, the notary does not receive the data from the transaction but can validate that the transaction took place. Two peers are always guaranteed to see the exact same version of the transactions they share. When a party receives a transaction from a peer they verify the signature is valid and that it is contractually valid before signing it, returning the signed version and committing it to storage.

The contract code is only run by the parties involved in a transaction and optionally a notary. Contracts run in a deterministic JVM creating a flexible development environment.

Conclave is an SGX SDK developed by R3, the company behind the Corda platform. It provides a higher level API for intel SGX which allows JVM bytecode to be executed in an enclave. There is currently no complete integration of Conclave in the Corda flow, although one is planned. As Conclave is a Java API it can be used by Corda DApps, meaning that one can write private contracts that will run in a SGX enclave.

Requirements	Platform Compatibility
Verifiable Transactions	Partial transactions are only verified by the parties involved and notaries
Private Transactions	Yes, through Conclave transactions can be verified without the details being visible
Scalable	Yes, 6300 TPS
Immutable Transactions	Yes, the involved parties and notary ensure ledger integrity
Flexible Governance	Yes, as there is no central ledger, governance of individual ledgers is flexible
Group Security	Partial, each ledger is protected by a small group of only relevant parties
Production Readiness	Corda is production ready and has an enterprise version. At time of writing Conclave is still in Beta.

Additional Considerations	
Ease of Development	The JVM gives good development flexibility. However the lack of integration may require work by a development team to get Conclave and Corda off the ground
Ease of Deployment	Good Corda is a very mature platform with a well documented deployment process and there is a guide to running conclave on linux
Flexibility of Deployment	Somewhat, deployment of Conclave requires SGX enabled hardware. SGX hardware is currently offered by Microsoft Azure, IBM Cloud & Alibaba cloud. Corda could be deployed separately on generic hardware as conclave and Corda are decoupled.
Requires Crypto payment for transactions	No

Chapter 3: Zero Knowledge Platforms

Zero knowledge proofs are mathematical cryptographic proofs that enable a party to prove that they know a value without revealing that value to a verifier.

Zero knowledge proofs have been heralded in the public blockchain space as solving data and transaction privacy issues and underpin public networks such as Zcash to allow parties to transact without publicly revealing the details of their transaction.

Some zero knowledge proof cryptography schemes allow for Turing complete proofs meaning that any computer program can be written with another party being able to verify a correct output without seeing the details of the program inputs. This means that we can use these programs as smart contracts.

This presents a number of advantages:

- We can build a smart contract like system where details are kept private from the wider network.
- The proving programs can be run once with the output being validated by everyone.
- Since validation is cheap there is a potential computational saving here vs a mechanism like the Ethereum Virtual Machine where the program is run by all parties to verify a transaction's validity.
- Mechanisms such as zk rollups give an additional performance benefit.

Considerations

Security

This is a very experimental and diverse area of research where novel cryptographic techniques are already used to protect assets in public blockchains. The complexity of ZKPs can lead to vulnerabilities: a vulnerability that enabled counterfeiting was identified and patched in zcash. Some mechanisms require a "trusted setup" where the creator of a circuit (smart contract like program) has a secret key which could be used to create fake proofs, in these mechanisms users must trust that the creator destroyed this secret key.

Performance

Performance with zero knowledge proofs is not straightforward, and we must consider a number of areas:

- Time to prove (run once offline)
- Time to validate a proof (assumed run by all validators)
- Size of the proof
- Circuit size.

Each of these elements depends on the proving scheme selected.

Portability

Zero knowledge proofs can be run on generic hardware, operating systems and infrastructure.

3.1 The Baseline Protocol

The Baseline Protocol is an open source project which aims to enable organizations to synchronize their private business processes and utilize the main Ethereum public net to enable event order and immutability of these processes.

The project has opened up a set of tools and packages to utilize the protocol. In order for parties to communicate they must set up a workflow by creating a custom zkSNARK circuit and a baseline protocol verifier contract that verifies that proofs have run through this circuit. The verifier contract is published to the public chain. When parties participate in this workflow they create a proof conforming to the circuit which is then verified on the public chain.

Baseline has connectors to integrate directly with local systems of record (Mongo, Oracle, SAP, etc). For defined workflows whenever a record is updated in one of these systems it will synchronize with other parties and the update will be validated by the circuit.

Requirements	Platform Compatibility
Verifiable Transactions	Yes, verified by public chain SNARKS verifier contract
Private Transactions	Yes, details of transactions not submitted to the blockchain
Scalable	No, Dependency on mainnet limits the solution ~13tps at time of writing. Transactions could be grouped but this will have an impact on verifiability of transactions
Immutable Transactions	Yes, transaction state is recorded on the mainnet. Actual details kept in local systems of record.
Flexible Governance	Yes, workgroups defined and managed on mainnet
Group Security	Yes, transactions validated by mainnet
Production Readiness	No documentation can be found of Baseline being used in production however ZK-SNARKS are used for production systems

Additional Considerations	
Ease of Development	The tooling around Baseline looks straightforward, however the requirement to write circuit code for some use cases makes development more challenging and puts a lot of pressure on the circuit code
Ease of Deployment	Good, tools have been created to generate and deploy smart contracts
Flexibility of Deployment	Very good, Can be deployed on generic hardware.
Requires Crypto payment for transactions	Yes

3.2 The Aztec Protocol

The Aztec protocol enables private transactions on public blockchains. In theory Aztec can be implemented on any blockchain capable of general purpose computation.

Currently the Aztec SDK supports the Ethereum Mainnet. Similar to Baseline, Aztec uses a verification contract to validate proofs for each spend. The protocol also supports custom assets which mimic ERC-20 contracts, this allows us to create a custom token on the mainnet and retain privacy.

Currently each Aztec transaction is also an Ethereum transaction with a limit of around 13 transactions per second. However Aztec plans to achieve scalability through zk-rollup allowing hundreds of transactions to be batched into a single transaction.

There are drawbacks to this method:

- Although hundreds of transactions can be processed at once there is a wait for transactions to accumulate before submitting so there may be large latency for transactions.
- The latency may make it susceptible to double spend where someone moves the funds before the batch containing their transaction is submitted.
- ZK Rollups are not currently available. However they are part of Aztec 2 with mainnet support planned for November.

Requirements	Platform Compatibility
Verifiable Transactions	Yes
Private Transactions	Yes
Scalable	Currently no however in the near future yes through zk rollups
Immutable Transactions	Yes verified by public net
Flexible Governance	No, zk-asset does not support easy customisation
Group Security	Yes secured through mainnet
Production Readiness	Available on mainnet since February

Additional Considerations	
Ease of Development	Friendly SDKs with limited customisation. Base features appear to be easy to use
Ease of Deployment	Good, Contract deployment scripts are open source
Flexibility of Deployment	Very Good, can be deployed on generic hardware
Requires Crypto payment for transactions	Yes

appliedblockchain

appliedblockchain.com

info@appliedblockchain.com

WHO WE ARE

Gartner

GLOBAL TOP 20 BLOCKCHAIN CONSULTING FIRM 2017-2020

Applied Blockchain builds enterprise grade applications with increased trust and data privacy for global companies and startups

Our background

Founded in 2015 with the vision of helping companies solve real world problems using confidential computing technologies and blockchains.

Our experience

Over the past 5 years we've been selected by some of the largest global organisations in financial services, energy, trading, shipping, automotive, aviation, telecoms and government.

Notable recognition

Gartner has recognised Applied Blockchain as a global leader in blockchain consulting in 2017-2020.

Forbes Bloomberg VentureBeat

"We did the first product derivative trade on blockchain together with our partner Applied Blockchain"

Ben van Beurden
CEO, Shell

Clients include:

Shell, Lloyd's Register, Bank of America, vodafone, SITA, KLM, TOYOTA, emsurge, nuggets, UNITED NATIONS, Travel Ledger

KYC, KYS, Compliance

Assets, Commodities Trading, Settlement

Credit Risk Management

SOLUTIONS

Supply Chain Management and Assurance

Invoice and Payment Tracking

Reduction in Product Counterfeit

appliedblockchain

applied-blockchain

@AppBlockchain_

@appblockchain


appliedblockchain