An attempt to give the most abstract possible definition of a blockchain.

1 BlockChain

Given a set S, let $\textsc{List}(S)$ and $\textsc{Set}(S)$ be the sets of all finite lists and all finite sets of elements of S, respectively. Given $L \in \textsc{List}(S)$, we use notation $|L|$ to refer to the number of elements in L, and notation $L[i]$ to refer to the i-th element in L, where $i \in \{1, \dots, |L|\}$. From now on, assume that Σ is a finite alphabet, and that $\mathbf{B} \subseteq \Sigma^*$ is the set of all possible blocks. Moreover we extend the definition of $\subseteq$ such that :

$$\forall S \in \textsc{Set}(B), \forall L \in \textsc{List}(B), L \subseteq S \Leftrightarrow \forall i \in \{1, \dots, |L|\}, L[i] \in S$$

Definition 1. *A validation rule is a function $V : \textsc{List}(\mathbf{B}) \to \textsc{Set}(\mathbf{B})$*

Intuitively V is a function taking a list L of block as input, and returning the set of blocks that could be added to L to produce a valid blockchain.

Definition 2. *Let $G \in \textsc{List}(\mathbf{B})$ be non-empty, and V be a validation rule. Then a list $L \in \textsc{List}(\mathbf{B})$ is a validated chain with respect to (G, V) if:*

1. *$|G| \leq |L|$ and $L[i] = G[i]$, for every $i \in \{1, \dots, |G|\}$.*
2. *$L[1] \in V([\,])$ and $L[i+1] \in V([L[1], \dots, L[i]])$, for every $i \in \{1, \dots, |L| - 1\}$.*

List L in this definition is a valid chain according to the validation rule V and the lists G of genesis blocks (whose role is to provide the blocks to startup the system). Let $\textsc{Log}(G, V)$ be the set of validated chains with respect to (G, V).

Definition 3. *Let $G \in \textsc{List}(\mathbf{B})$ be non-empty, and V be a validation rule. Then $\textsc{Log}(G, V)$ is safe if for every $L \in \textsc{Log}(G, V)$ such that every $b_1, b_2 \in \mathbf{B}$ such that $b_1 \neq b_2$:*

$$V([L[1], \dots, L[|L|], b_1]) \cap V([L[1], \dots, L[|L|], b_2]) \quad = \quad \emptyset$$

Intuitively, in order to be secured V should depend on the last block b that is included in the blockchain.

Definition 4. *Let P be a set of players and K_T a function :*

$$K_T : P \times [\![0; T]\!] \times \mathbb{N} \to \textsc{Set}(\mathbf{B} \times [0; 1])$$

Then (P, K_T) is a valid knowledge representation if :

$$\begin{gathered}
\forall p \in P, \forall t \in [\![0; T]\!], (b, \alpha) \in K_T(t, 0, p) \implies \alpha = 1 \vee \alpha = 0 \\
\forall p \in P, \forall t, t' \in [\![0; T]\!], t' \geq t, \forall b \in \mathbf{B}, (b, 1) \in K_T(t, 0, p) \implies (b, 1) \in K(t', 0, p) \\
\forall p \in P, \forall t \in [\![0; T]\!], \forall \delta \in \mathbb{N}, \forall b \in \mathbf{B}, (b, 1) \in K_T(t, 0, p) \implies (b, 1) \in K(t, \delta, p) \\
\forall p \in P, \forall t \in [\![0; T]\!], \forall \delta, \delta' \in \mathbb{N}, \delta' \geq \delta \implies \forall (b, \alpha) \in K_T(p, t, \delta), \exists (b, \alpha') \in K_T(p, t, \delta'), \alpha' \geq \alpha
\end{gathered}$$

Notation. *$\forall p \in P, \forall t \in [\![0; T]\!]$ we denote*

$$K_T(p, t) = \{b | (b, 1) \in K_T(p, t, 0)\}$$

Definition 5. *Let $T, T' \in \mathbb{N}$ such that $T > T'$ we say that $K'_{T'}$ extend K_T if*

$$\forall p, K_T(p, T) = K'_{T'}(p, T)$$

Definition 6. *Let $\preceq_{G,V,t}$ be a total preorder over $LOG_{G,V}$:*

$$\forall L_1, L_2, L_3 \in LOG_{G,V}, L_1 \preceq_{G,V,t} L_2 \wedge L_2 \preceq_{G,V,t} L_3 \implies L_1 \preceq_{G,V,t} L_3$$
$$\forall L_1, L_2 \in LOG_{G,V}, L_1 \preceq_{G,V,t} L_2 \vee L_2 \preceq_{G,V,t} L_1$$

A block chain protocol over $LOG_{G,V}$ is a function noted $\preceq_{G,V}$ such that:

$$\forall t \in \mathbb{N}, \preceq_{G,V} (t) = \preceq_{G,V,t}$$

where $\preceq_{G,V,t}$ is a total preorder over $LOG_{G,V}$

Remark. *$\preceq_{G,V}$ can be seen as the rules in case of fork and new block.*

Definition 7. *Considering $LOG_{G,V}$ the set of validated chains with respect to (G, V), (P, K_T) a valid knowledge representation and $\preceq_{G,V}$ a block chain protocol. We denote $S_{t,p}$ where $t \in [\![0, T]\!]$ and $p \in P$ the set:*

$$S_{t,p} = \{L | L \in LOG_{G,V} \wedge L \subseteq K_T(p, t)\}$$

We call a BlockChain at time $t \in [\![0, T]\!]$ for user $p \in P$ noted $BC_{t,p}$ a list such that:

$$BC_{t,p} \in S_{t,p} \wedge \forall L \in S_{t,p}, L \preceq_{G,V,t} BC_{t,p}$$

Remark. *Intuitively the blockchain for a user p at a time t is one of the best chain he fully knows regarding the protocol function and the validity at time t (time-stamping).*

Definition 8. *Considering $LOG_{G,V}$ the set of validated chains with respect to (G, V), (P, K_T) a valid knowledge representation. We denote α^* the function*

$$\mathbb{N} \times LOG_{G,V} \times P \to [0, 1]$$

such that :

$$\alpha^*(\delta, L, p) = max\{\alpha | \exists b \in \mathbf{B}; (b, \alpha) \in K_T(p, T, \delta) \cap V(L)\}$$

We said that $LOG_{G,V}$ is alive regarding (P, K_T) if:

$$\exists p \in P, \exists L \in LOG_{G,V}, L \subseteq K_T(p, T) \wedge K_T(p, T) \cap V(L) = \emptyset \wedge \lim_{\delta \to +\infty} \alpha^*(\delta, L, p) = 1$$

2 draft

Definition 9. *Considering (P, K_T) a valid knowledge representation, $LOG_{G,V}$ the set of validated chains with respect to (G, V) alive, and $\preceq_{G,V}$ a block chain protocol. Let $L \in LOG_{G,V}$ we note the probabilty that $L \subseteq B_{T+\delta,p}$*

Definition 10. *Considering $LOG_{G,V}$ the set of validated chains with respect to (G, V), (P, K_T) a valid knowledge representation. A block chain protocol $\preceq_{G,V,T}$ is said to be ageing-secured if*

$$\forall p \in P, \forall T_0 < T, \forall t, t' \leq T, B_{t,p} \subseteq B_{T_0,p}, B_{t',p} \subseteq B_{T_0,p}$$
$$t \leq t' \implies \forall T_1 \geq T_0, \mathbb{P}(B_{t,p} \subseteq B_{T_1,p}) \geq \mathbb{P}(B_{t',p} \subseteq B_{T_1,p})$$