బిట్ కాయిన్: ప్రతీ ఒక్కరికీ సరి సమానమ ైన ఎలకారా నికి కాష్ సిసరమ్

సటోషి నక్మోటో
satoshin@gmx.com

www.bitcoin.org

సారాంశాం - ఎలకారా నిక్ కాష్ అనే ఫీచర్ ప◌ూరిగా పీర్-టు-పీర్ వెర్షన్ ద్వారా ప్రతి సభ్యానికి ఆన్ ల ైన్ చెల్లాంప◌ులు ఆరిక్ సాంసి ద్వారా వెళ్లక◌ాండవ చేస◌ి ◌ాంద◌ి. తాంతేకాక◌ాండవ ఈ ఎలకారా నిక్ కాష్ అనే ఫీచర్ ద్వారా ఒక్ పారటర న◌ాండి మరొక్ పారటరకి నగద్ ప◌ాంప్డవనికి అన్మతిస◌ి ◌ాంద◌ి. అయితే డబయల్ ఖర్చున్ నిరోధాంచడవనికి నమమక్మ ైన మూడోపాక్షం అవసర్మ ైనప◌ుడు ప్రధవన ప్రయోజనవలు కోలపుయే ప్రమాదాం ఉాంద◌ి. ఇక్కడ డిజిటల్ సిగనేచ◌ర్ క ◌ాంత భాగాం ప్రిష◌ాకరాలన్ తాంద◌ిసా యి. మేమయ పీర్-టు-పీర్ నెట్ వర్క ని ఉప్యోగాంచి డబయల్ ఖర్చు సమసాక◌ు ప్రిష◌ాకరానీ ప్రతిపాద◌ిస◌ి నవేమయ. నెట్ వర్క ట ైమ్ సార ◌ాంప్ లావాద◌ేవీలు హ్యాష్-ఆధవరిత ప◌ూా ఫ్-ఆఫ్-వర్క చెయిన్ లప హ్యాష్ చేయడాం జర్చగయత ◌ాంద◌ి. తద్వారా, ప◌ూా ఫ్-ఆఫ్- వర్క న్ మళ్లల చేయక◌ాండవ ఎవా◌ార్ మా◌ర్లేని రికార్చు న్ ఏ◌ర్ర్చస◌ి ◌ాంద◌ి. లాాంగెస్టర చెయిన్ జరిగిన సాంఘటనలక◌ు ర్చజువుగా మాతరమే కాక◌ాండవ, ఇద◌ి అతిపెదద సీపీయయ న◌ాండి వచ్చిాందని ర్చజువు చేస◌ి ◌ాంద◌ి. సీపీయయ ప్వర్ లప ఎక◌ుకవ భాగాం నెట్ వర్క ప ై ద్వడి చేయడవనికి సహక్రాంచని నోడ లచే నియాంతిరాంచబడిఉాంటాంద◌ి. తాంద్వలల, అవి పొ డవైన చైన్ మరియయ అవుట్ పేస్ట అటాక్ర లన్ ఉతులి చేసా యి. నెట్ వర్క క◌ు క్నీస నిరామణాం అవస◌ారం. మేసేజ్ లు ఉతిమ ప్రయతాం పార తిష్ఠిక్న ప్రసా◌ార్ం చేయబడతవయి. నోడ లు తమ ఇష◌ార న్సా◌ార్ం నెట్ వర్క న్ విడిచిపెటరవచ◌ు మరియయ తిరిగి చేర్వచ◌ు. అవి పో యినప◌ుడు ఏమి జరిగాందనే ద్వనికి ర్చజువుగా లాాంగ్ ప◌ూా ఫ్-ఆఫ్-వర్క చైన్ న్ మనక◌ు తాంద◌ిసా యి.

1. పరిచయం

ఇాంటరేట్ లప వాణిజాం, వాాపారానికి సాంబాంధాంచి ఎలకారా నిక్ చెల్లాంప◌ులన్ పార సెస్ట చేయాలాంటే మనాం కృితాంగా థ◌ర్ పారటరగా ఉనే ఆరిక్ సాంసిలప ై ఆధవర్పడక తప◌ుద్. పాంద్క◌ాంటే సిసరమ్ చవలా లావాద◌ేవీలక◌ు తనక◌ు అన్గయణాంగా మార్చుక◌ుని, తనలప సేవ్ చేస్క◌ునేప◌ుటికీ, ఇద◌ి ఇప◌ుటికీ టరస్టర ఆధవరిత మోడల్ యొక్క సాాభావిక్ బలహీనతలతో బాధప్డుతోాంద◌ి. వివాద్వలక◌ు మధావరితాం వహ ◌ాంచక◌ాండవ ఆరిక్ సాంసిలు తప్పాంచ్కోలేవు కాబటిర ప◌ూరిగా రివర్బయల్ లావాద◌ేవీలు నిజాంగా సాధాం కాద్. మధావరితాం లావాద◌ేవీ వాయాలన్ పెాంచ్త ◌ాంద◌ి. ఇద◌ి క్నీస ఆచర్ణవతమక్ లావాద◌ేవీల ప్రిమాణవనీ ప్రిమితాం చేస◌ి ◌ాంద◌ి. చినే సాధవర్ణ

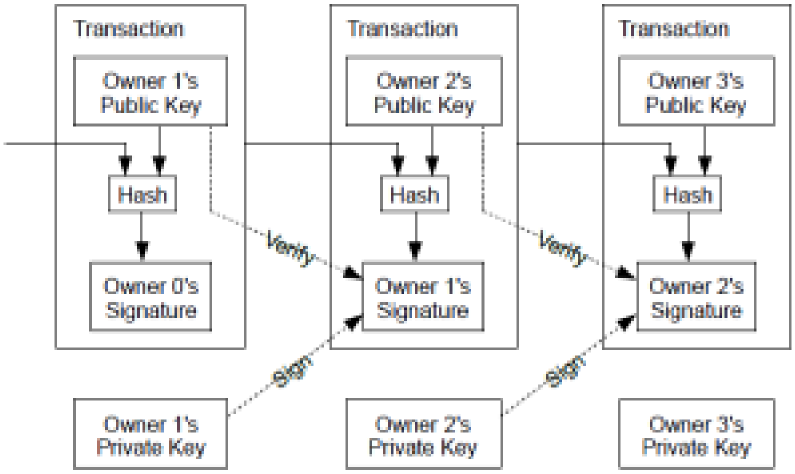
లావాద్ేవీలక్ు అవకాశాం తగయు త ాంద్ి. అనేాంటికి మిాంచి నవన్-రివర్బయల్ సేవలక్ు రివర్బయల్ కాని చెల్లాంప్ులు చేసే సామరి ాని కోలపువడాంలప విస్సృత ఖర్చు ఊాంటూాంద్ి. తిరోగమనాం యొక్క అవకాశాంతో, విశ్ాాసాం యొక్క అవస ార్ం వాాపిస్ి ాంద్ి. వాాపార్చలు తమ వినియోగద్వర్చల ష్టల జాగరతిగా ఊాండవల్. పాంద్క ాంటే ఒకోకసారి వినియోగద్వర్చలు వారికి ద్వనిక్ ాంటే ఎక్ుకవ సమాచవ ార్ం కోసాం ఇబబాంద్ి

పెడుత ాంటార్చ. ఇలాాంటి సమయాాంలప మోసాం యొక్క శ్ ాతాం అనివా ార్మ ైనద్ిగా తాాంగటక్రాంచబడుత ాంద్ి. ఫిజిక్ల్ క్రెన్ని ఉప్యోగిాంచడాం ద్వారా ఈ ఖర్చులు మరియయ చెల్లాంప్ు వాాకిగతాంగా నివారిాంచబడతవయి, అయితే విశాసనీయ పోక్షం లేక్ాండవ కమ్యానికనషన్ ఛవనెల్ లప చెల్లాంప్ులు చేయడవనికి ఎలాాంటి యాాంతవర ాంగాం లేద్.

అయితేఇలాాంటిసమయాాంలప విశాసనీయతక్ు బద్లుగా కిరపరోగారఫిక్ ర్చజువుపైెఆధవర్పడిన ఎలకారానిక్ చెల్లాంప్ు వావసి చవలా అవస ార్ం. నమమకమ ైన థ ుర్ పారటర అవస ార్ం లేక్ాండవ ఏద్ ైనవ ఇదదర్చ సిదధాంగా ఉనే పారటరలు ఒక్రితో ఒక్చ నేర్చగా లావాద్ేవీలు జర్చప్ుక్ునేాంద్క ు వీలు క్ల్ుస్ి ాంద్ి. రివ ర్ చేయడవనికి క్ుదర్ని లావాద్ేవీలు వికనరతలన్ మోసాం న్ ాండి కాపాడతవయి. క నోలుద్వర్చలన్ ర్క ిాంచడవనికి సాధవర్ణ ఎసో రో మ కానిజమ్ లన్ స్లభ్ ాంగా అమలు చేయవచ్ు. ఈ పేప్ర లప, లావాద్ేవీల యొక్క ల క్కలన్ తాాంద్ిాంచేాంద్క ు పీర్-టు-పీర్ డిసిరిబూాట డ ట ైమ్ సార ాంప్ స ార్ర్ ని ఉప్యోగిాంచి డబయల్ ఖర్చ సమసాక్ు ప్రిష్ాకరానీ మేమయ తాాంద్ిస్ి నవేమయ. అటాక్ర నోడ లు సమిషిరగా ఎక్ుకవ సీపీయయ శ్కిని నియాాంతిరస్ి నేాంత వర్క ు సిసరమ్ స్క ిాంగా ఊాంటూాంద్ి.

2. లావాదేవీలు

మేమయ ఎలకారా నిక్ కాయిన్ ని డిజిటల్ సిగనేచర్ చెయిన్ గా మారనుశ్ాం. ప్రతి యజమాని మయన్ని లావాద్ేవీకి సాంబాంధాంచిన హ్యాష్ పై డిజిటల్ సాంతక్ాం చేయడాం మరియయ తద్ప్రి యజమాని యొక్క ప్బిల క్ కీపై డిజిటల్ సాంతక్ాం చేయడాం ద్వారా కాయిన్ ని తద్ప్రి ద్వనికి బద్ిలీ చేసా ర్చ. మేనేజ్ మ ాంట్ యొక్క చెయిన్ న్ ధృవీక్రాంచడవనికి చెల్లాంప్ుద్వర్చ సాంతకాలన్ ధృవీక్రాంచవచ్ు.



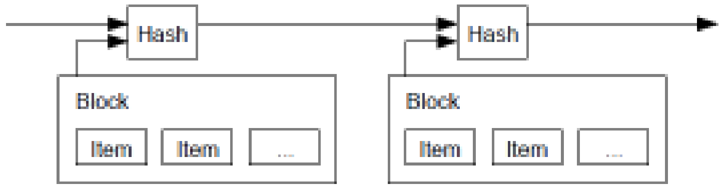
అయితే ఇక్కడ సహజాంగా వచే సమసా ఏంటాంటే.. కాయిన్ ఓనర్ లప ఒక్కెన ఒక్ యజమాని రెండు సార్చల ఖర్చు చేశారా లేద్వ అనే విషయానీ చెల్లాంపుద్వర్చ ధృవీక్రాంచలేర్చ. ప్రతి లావాదేవీని రెటిరాంపు ఖర్చు కోసాం తనిఖీ చేసే విశాసనీయ కనాందర అధికారానీ లేద్వ మింట్ న్ ప్రిచయాం చేయడాం ఇక్కడ ఒక్ సాధవర్ణ ప్రిష్కారం. ప్రతి లావాదేవీ తరాాత, ఒక్ క తి కాయిన్ జారట చేయడవనికి కాయిన్ తప్పునిసరిగా మింట్ కు తిరిగి ఇవాబడుత ుంది. మింట్ న్ుండి నేర్చగా జారట చేయబడిన నవణేలు మాతరమే రెండింతలు ఖర్చు చేయబడవని నమయమతవర్చ. ఈ ప్రిష్కారంతో సమసా ఏమిటాంటే, మొతాం డబయబ వావసి యొక్క మింట్ న్ నడుపుత నే కంపెనీపై ఆధవర్పి ఉంటుంది, ప్రతి లావాదేవీ వారి ద్వారానే జర్గాల్, బ్యాంకు లాగా.

మయన్పి ఓనర్ లు మయన్పిలావాదేవీలపైసాంతకం చేయలేదని చెల్లాంపు గరహీత తెలుస్కోవడాం కోసాం మాకు ఒక్ మార్గం అవసరం. ఇాంద్కోసాం, మయాంద్గా జరిగిన లావాదేవీయే ప్రిగణించబడుత ుంది, కాబటిర మేమయ తరాాత రెటిరాంపు ఖర్చు చేసే ప్రయతవేల గయరించి ప్టిరాంచ్కోమయ. లావాదేవీ లేనటుల నిరాధ రించడవనికి ఏకైక్ మార్గం అనీ లావాదేవీల గయరించి తెలుస్కోవడమే. మింట్ ఆధవరిత మోడల్ లప, మింట్ అనీ లావాదేవీల గయరించి తెలుస్కుని, ఏది మయాంద్గా వచింద్ో నిర్ణయాంచ్కుటుంది. విశాసనీయ పోక్షం లేకుండవ దీనీ నివారించడవనికి, లావాదేవీలు తప్పునిసరిగా బహ ిరంగాంగా ప్రక్టించబడవల్ [1] మరియయ పాలగు నేవార్చ వార్చ సీక్రాంచబడిన క్రమాంలప ఒకన చరితరన్ తాంగటక్రాంచేంద్కు మాకు వావసి అవసరం. ప్రతి లావాదేవీ సమయాంలప, మ జారిటీ నోడ లు మొదట సీక్రాంచినటుల తాంగటక్రాంచినటుల చెల్లాంపుద్వర్చనికి ర్చజువు అవసరం.

3. ట ైమ్ సటాంప్ సర్వర్

ఇక్ మేమయ ప్రతిపాదించే ప్రిష్కరాలు ట ైమ్ సార ాంప్ సర్రర్ తో పార రంభాం అవుతవయి. ట ైమ్ సార ాంప్ సర్రర్ ట ైమ్ సార ాంప్ చేయవలసిన వస్ువుల బాల క న్ తీస్కు ని, వారి ప్తిరక్ లేద్వ యూజ్ నెట్ పో స్టర [2-5] వాంటి హ్యాష్ న్ విస్పృతాంగా

ప్రచ్రించడాం ద్వారా ప్ని చేస్ి ుంది. ట ైమ్ సార ాంప్ హ్యాష్ లపకి ప్రవేశాంచడవనికి, ఆ సమయాంలప డేటా తప్పునిసరిగా ఉనికిలప ఉందని ర్చజువు చేస్ి ుంది. ప్రతి ట ైమ్ సార ాంప్ ద్వని హ్యాష్ లప మయన్పి ట ైమ్ సార ాంప్ న్ క్లి ఉంటుంది, ఒక్ చెయిన్ న్ ఏర్పర్చస్ి ుంది, ప్రతి అదనపు ట ైమ్ సార ాంప్ ద్వని మయాంద్ ఉనే వాటిని బలపపేతాం చేస్ి ుంది.

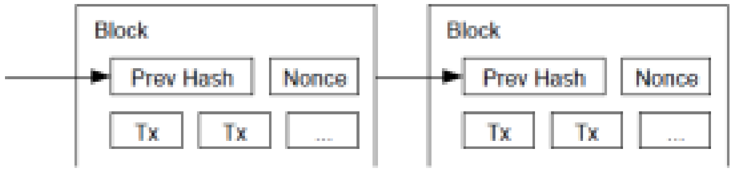


4

4. వ◌ర్ కు సంబంధ ◌ంచిన ఆధారాలు

పీర్-టు-పీర్ పార తిప్ది◌క్న ప◌ంపిణీ చేసిన ట ◌ైమ్ సార ◌ంప్ స◌ర్ర్ న్ అమలు చేస◌ంద్క◌ు, మేమయ వారి◌ ప్తిరక లేద్వ యూజ్ నెట్ పో స్టర ల క◌ంటే ఆడమ్ బాక్ యొక్క హ్యాష్ కాష్ [6] మాద◌ిరిగానే ప◌ూా ఫ్-ఆఫ్-వర్క సిసరమ్ న్ ఉప్యోగ◌ంచవల◌్ ఉ◌ంటుంద◌ి. SHA-256 హ్యాష్ చేయబడినప◌ుడు, హ్యాష్ అనేక స్నపే బిట్ లతో పార ◌ర౦భ్మయా విలువ కోస◌ం సాకన్ చేయడవనీ ప◌ూా ఫ్-ఆఫ్-వర్క ఉ◌ంటుంద◌ి. అవసర్మ ◌ైన స్నపే బిట్ ల సా◌ంఖాలప సగటు ప్ని తవలూక◌ు ఒకన హ్యాష్ ని అమలు చేయడ◌ం ద్వారా ధృవీక్రి◌ంచబడుత ◌ంద◌ి.

మా ట ◌ైమ్ సార ◌ంప్ నెట్ వర్క కోస◌ం, బాల క్ హ్యాష్ కి అవసర్మ ◌ైన స్నపే బిట్ లన్ తా◌ంద◌ి◌ంచే విలువ క్నొనబడే వర్క◌ు బాల క్ లప నవన◌్ న్ హె◌ంచడ◌ం ద్వారా మేమయ ప◌ూా ఫ్-ఆఫ్-వర్క న్ అమలు చేసా మయ. సీపీయయ ప్రయతేం ప◌ూా ఫ్-ఆఫ్-వర్క న్ సా◌ంతృపి ప్రచడవనికి ఖర్చు చేసిన తరాత, ప్నిని మళ్లల చేయక◌ా◌ండవ బాల క్ ని మా◌ుర్లేర్చ. తర్చవాతి బాల క్ లు ద్వని తరాత బా◌ంధి◌ంచబడినా◌ంద్న, బాల క్ న్ మారను ప్నిలప ద్వని తరాత అనీ బాల క్ లన్ మళ్లల చేయడ◌ం ఉ◌ంటుంద◌ి.



మరోవైప◌ు మ జారిటీ నిర్ణయ◌ం పార తినిధవానీ నిర్ణయ◌ంచే సమసాన్ క◌ూడవ ప◌ూా ఫ్-ఆఫ్-వర్క ప్రిష్కరిస◌ి ◌ంద◌ి. మ జారిటీ ఒక ఐపీ-అడరస్ట- ఒక వోటు పై ఆధవర్ప్డి ఉ◌ంటే, అనేక ఐపీలన్ కనటాయి◌ంచగల్గిన ఎవరైనవ ద్వనిని తవర్చమార్చ చేయవచ◌ు. ప◌ూా ఫ్-ఆఫ్-వర్క తప◌ునిసరిగా ఒక-సీపీయయ-ఒక-ఓటు. మ జారిటీ నిర్ణయ◌ం పొ డవైన చెయిన్ ల ద్వారా పార తినిధ◌ం వహ స◌ి ◌ంద◌ి, ఇ◌ంద్లప గొప◌ు ప్ని కోస◌ం పెటుర బడి పెటిరనటుల ర్చజువు ఉ◌ంద◌ి. సీపీయయ ప్వర్ లప ఎక◌ుకవ భాగ◌ం నిజాయితీ గల నోడ లచే నియ◌ంతిర◌ంచబడితే, నిజాయితీ గల చెయిన్ అత◌ంత వేగ◌ంగా అభివృద◌ిధ చె◌ంద్త ◌ంద◌ి, అద◌ే సమయ◌ంలప ఏద్◌ైనవ పో టీ చెయిన్ లన్ అధిగమిస◌ి ◌ంద◌ి. గత బాల క్ న్ సవరి◌ంచడవనికి, ద్వడి చేసే వాకి బాల క్ యొక్క ప◌ూా ఫ్- ఆఫ్-వర్క న్ మరియయ ద్వని తరాత అనీ బాల క్ లన్ మళ్లల చేయాల్. ఆ నిజాయితీ గల నోడ ల ప్నిని ప్టుర క◌ుని, అధిగమి◌ంచవల్. తద్ప్రి బాల క్ లు జోడి◌ంచబడినా◌ంద్న నెమమద◌ిగా ద్వడి చేసే వాకి కాచ్ అప్ అయ్యే సా◌ంభావాత విప్రటతా◌ంగా తగిపో త ◌ందని మేమయ తరాత ద్వనీ వివర్ణవతమక◌ంగా చూప◌ుతవమయ.

హ్యా◌ుర్ వేర్ వేగానీ హె◌ంచడ◌ం, కాలక్రమేణవ నోడ లన్ అమలు చేయడ◌ంలప వివిధ ర్కాల ఆసకిని భ్రటి చేయడవనికి, ప◌ూా ఫ్- ఆఫ్-వర్క క్ష◌ార లు గ◌ంటక◌ు సగటు బాల క్ ల సా◌ంఖాన్ లక్షా◌ంగా చేస్క◌ుని క్ద◌ిలే సగటు ద్వారా

నిర్ణయాించబడతవయి. అవి చవలా వేగాంగా ఉతుతి చేయబడితే, క్షరాం పెర్చగయత ొాంద్ి.

5. నెట్ వ ర్

నెట్ వర్క ని ర్న చేసేాంద్కు దశలు కిరాంద్ి విధాంగా ఉనవేయి:

1) క తి లావాద్ేవీలు అనీ నోట్ లక ు ప్రసా ార్ం చేయబడతవయి.

2) ప్రతీ నోడ క తి లావాద్ేవీలన్ బాల క్ లప ఉాంచ్తు ొాంద్ి

3) ప్రతి నోడ బాల క్ కోసాం క్షరమ ైన ప్ ూా ఫ్-ఆఫ్-వర్క న్ క్నొగనడాంలప ప్ని చేస్ి ొాంద్ి.

4) ఒక్ నోడ ప్ ూా ఫ్-ఆఫ్-వర్క ని క్నొగనేప్ ుడు, అద్ి బాల క్ లపని అనీ నోడ లక ు ప్రసా ార్ం చేస్ి ొాంద్ి.

5) నోడ్ లపని అనీ లావాద్ేవీలు చెలుల బాటు అయేావి మరియయ ఇప్ ుటికన ఖర్చు చేయనటలయితేనే బాల క్ న్ తాంగటక్రిసా యి. 6) నోడ లు చెయిన్ లప తద్ప్ర బాల క్ న్ ార్పొాంద్ాించడాంలప ప్ని చేయడాం ద్వారా బాల క్ కి తమ తాంగటకారానీ తెల్యజనసా యి, ఆమోద్ాించబడిన బాల క్ యొక్క హ్యాష్ న్ మయన్పిు హ్యాష్ గా ఉపోయగిసా యి.

నోడ లు ఎలలప్ ుడూ పొ డవైన చెయిన్ న్ సరైనద్ిగా ప్రిగణిసా యి. అద్ే సమయాంలప ద్వనిని పొ డిగాించడాంలప ప్ని చేసూ నే ఉాంటాయి. రెాండు నోడ లు తద్ప్ర బాల క్ యొక్క విభినే సాంసకర్ణలన్ ఏక్కాలాంలప ప్రసా ార్ం చేసి, క నీ నోడ లు మయాంద్గా ఒక్టి లేద్వ మరొక్టి తాంద్కోవచ ు. అలాాంటప్ ుడు, వార్చ తాంద్క ునే మొదటి ద్వనిలప ప్ని చేసా ర్చ, కానీ అద్ి ఎక్ ుకవ కాలాం మారితే ఇతర్ శ ాఖన్ సేవ్ చేయాల్ ్ ఉాంటుాంద్ి. ప్ని యొక్క తద్ప్ర ర్చజువు క్నొగనబడినప్ ుడు మరియయ ఒక్ శ ాఖ పొ డవుగా మారినప్ ుడు ట ై విరిగిపో త ొాంద్ి; ఇతర్ బార ాంచ్ లప ప్ని చేస్ి నే నోడ లు తరాాత పొ డవైన వాటికి మార్చతవయి.

క తి లావాద్ేవీ ప్రసారాలు తప్ునిసరిగా అని నోడ లన్ చేర్చకోవాల్్న అవసారం లేద్. అవి చవలా నోడ లన్ చేర్చక్ునేంత కాలాం, అవి చవలా కాలాం మయాంద్ బాల క్ లపకి వసా యి. బాల క్ బార డ కాస్టర లు ప్డివో యిన సాంద్ేశాలన్ క్ూడవ సహ ాంచగలవు. నోడ బాల క్ ని తాంద్కోవ్ తే, అద్ి తద్ప్ర బాల క్ ని సీాక్రాంచినప్ుడు మరియయ అద్ి మిస్ట అయినటుల గయరిాంచినప్ుడు ద్వనిని అభ్ారిస్ి ాంద్ి.

6. ప్రో త్ాాహకాలు

ల క్క ప్రకాారం, బాల క్ లప మొదటి టార నవా క్షన్ బాల క్ సృషిరక్ర్ి సొాంతద్ైన క తి కాయిన్ ని పార ారంభాంచే ప్రతేాక్ లావాద్ేవీ. ఇద్ి సెట్ వర్క క్ు మదదత ఇవాడవనికి నోడ లక్ు పోర తవ్హాని తాంద్ిస్ి ాంద్ి.

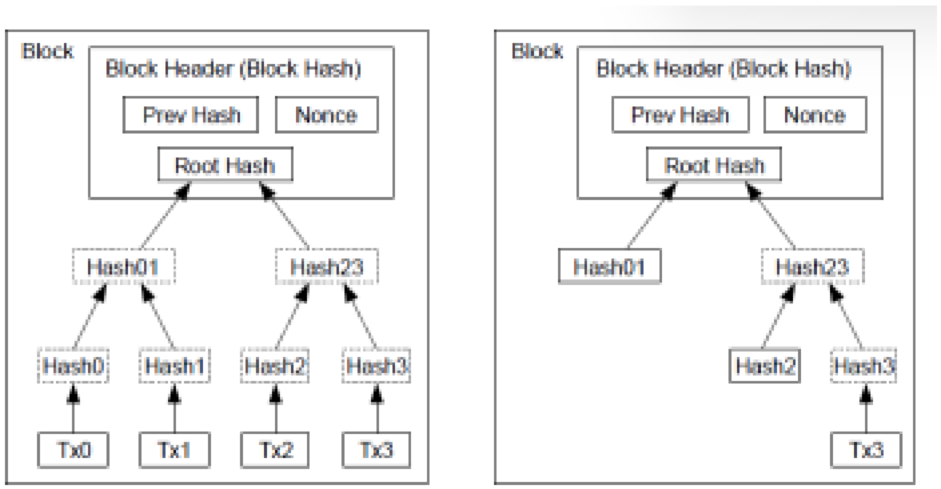
తాంతేకాక్ుాండవ పార ారంభ్ాంలప కాయిన్ లన్ ప్ాంపిణీ చేయడవనికి ఒక్ మారాు నీ తాంద్ిస్ి ాంద్ి.
పాంద్కాాంటే వాటిని జారట చేయడవనికి కనాందర అధికాారం లేద్. క తి కాయిన్ సిర్మ ైన మొతాంలప బాంగాారం చలామణికి జోడాంచడవనికి వనర్చలన్ వెచ్ాంచే బాంగార్చ మ ైనర్చల వల ఊాంటూాంద్ి. మా విషయాాంలప, ఇద్ి సీపీయయ సమయాం మరియయ విద్ాత్ ఖర్చు అవుత ాంద్ి.

లావాద్ేవీ ఫీజుతో క్ూడవ పోర తవ్వక్ నిధ్లు పొాందవచ్ు. లావాద్ేవీ యొక్క అవుట్ ప్ుట్ విలువ ద్వని ఇన్ ప్ుట్ విలువ క్ాంటే తక్ుకవగా ఊాంటే, తేడవ అనేద్ి లావాద్ేవీని క్లి ఉనే బాల క్ యొక్క పోర తవ్వక్ విలువక్ు జోడాంచబడే లావాద్ేవీ ర్చస్మ య. మయాంద్గా నిర్ణయాాంచిన సాంఖాలప కాయిన్్ చలామణిలపకి వచిున తరాాత, పోర తవ్వక్ాం ప్ూరిగా లావాద్ేవీల ర్చస్మ యలక్ు మార్చత ాంద్ి మరియయ ప్ూరిగా దరవోలబణాం లేక్ుాండవ ఊాంటూాంద్ి.

నోడ లన్ నిజాయితీగా ఊాండేలా పోర త్ా ాంచడాంలప పోర తవ్వక్ాం సహాయపడవచ్ు. అతవాశతో ద్వడి చేసే వాకి అనీ నిజాయితీ గల నోడ ల క్ాంటే ఎక్ుకవ సీపీయయ పవర్ న్ సమీక్రాంచగలిగితే, అతన్ తన చెల్లాంప్ులన్ తిరిగి ద్ ాంగిల్ాంచడాం ద్వారా ప్రజలన్ మోసాం చేయడవనికి లేద్వ క తి కాయిన్్ న్ ూర్పొాంద్ాంచడవనికి ద్వనీ ఉప్యోగాంచ్కోవాల్్ ఊాంటూాంద్ి. వావసిన్ మరియయ అతని సాాంత సాంపద యొక్క చెలుల బాటున్ అణగద్ క్కడాం క్ాంటే, తాందరి క్ాంటే ఎక్ుకవ క తి నవణేలతో అతనికి అన్కూలాంగా ఊాండే నిబాంధనల ప్రకాారం ఆడటాం మరాంత లాభ్దయక్ాంగా ఊాండవల్.

7. డిస్క్ స్పేస్ ని తిరిగి ప్ ాందడం

కాయిన్ లపని తవజా లావాద్ేవీని తగినాంత బాల క్ ల కిరాంద ప్ూరిగా పెటిరన తరాాత, డిస్టక సిలానీ ఆద్వ చేయడవనికి ద్వని మయాంద్ ఖర్చు చేసిన లావాద్ేవీలన్ విసమరాంచవచ్ు. బాల క్ యొక్క హ్యాష్ న్ విచిునాం చేయక్ుాండవ ద్ీనీ స్లభ్తాారం చేయడవనికి, లావాద్ేవీలు మ రికల్ టీరలప హ్యాష్ చేయబడతవయి [7][2][5], బాల క్ యొక్క హ్యాష్ లప ూర్ట్ మాతరమే చే్ర్బడుత ాంద్ి. చెటుర యొక్క క మమలన్ క్తిరాంచడాం ద్వారా పాత బాల క్ులన్ క్ుద్ాంచవచ్ు. తాంతుర్త హ్యాష్ లన్ నిలా చేయవలసిన అవసాారం లేద్.



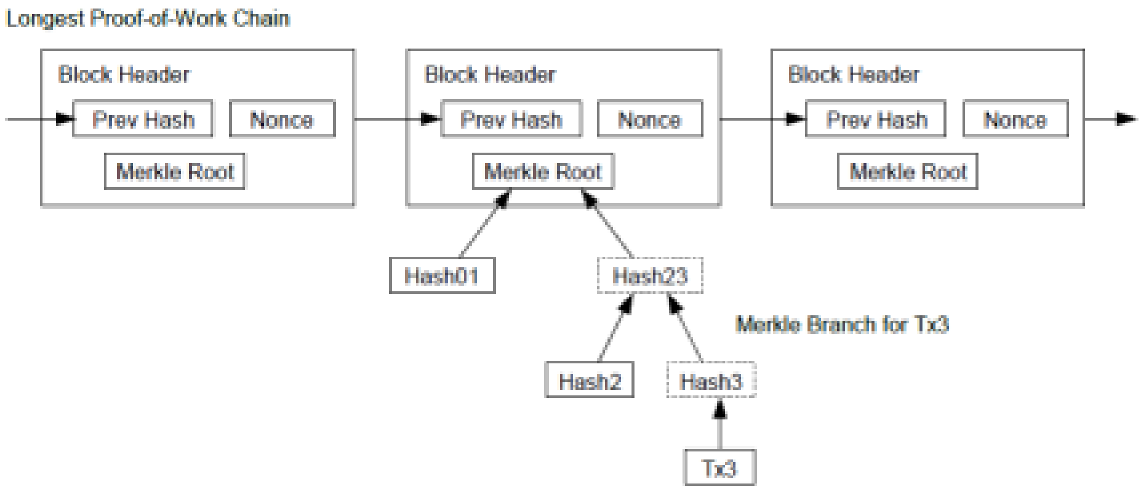
Transactions Hashed in a Merkle Tree　　　After Pruning Tx0-2 from the Block

బాల క న్ాండి Tx0-2 క్తిరాంప్ు తరాాత మ రికల్ టీరలప హ్యాష్ చేయబడిన లావాద్ేవీలు

లావాద్ేవీలు లేని బాల క హెడర్ ద్వద్వప్ు 80 బ ైట్ లుగా ఉాంటుాంద్ి. ప్రతి 10 నిమిష్ాలక్ు బాల క లు ఏరాటు అవుత నవేయి అని అన్క్ుాంటే, ఏడవద్ికి 80 బ ైటుల * 6 * 24 * 365 = 4.2MB ఏరాటు అవుతవయి. క్ాంప్ూాటర్ సిసరమ్ లు సాధవర్ణాంగా 2008 నవటికి 2GB RAMతో విక్రయాాంచబడుత నవేయి. మూర్ యొక్క చటరాం ఏడవద్ికి 1.2GB ప్రస్ి త వృద్ిధని అాంచనవ వేస్ి నేంద్న, బాల క హెడర్ లు తప్ునిసరిగా మ మరటలప ఉాంచబడినప్ుటికీ నిలా సమసా ఉాండక్ూడద్.

8. సర్ళంగా ఉండే పపమ ంట్ వెరిఫికేషన్

ప్ారి సెట్ వర్క నోడ ని అమలు చేయక ాండవ చెల్లాంప్ులన్ ధృవీక్రాంచడాం సాధామవుత ాంది. ఒక్ వినియోగదవ్రు పొ డవైన ప్ూఫ్-ఆఫ్-వర్క చెయిన్ యొక్క బాల క్ హెడర్ ల కాపీని మాతరమే ఉాంచ్కోవాల్. అతన్ తన వదద లాాంగ్ చెయిన్ న్ క్లి ఉనవడని విశాసాంచే వర్క్ు సెట్ వర్క నోడ లన్ ప్రశాంచడాం ద్వారా పొాందవచ్ు. లావాదేవీని బాల క్ కి లాంక్ చేసే మ రికల్ బార ాంచ్ న్ పొాందగలడు. ఇది ట మ్ సార ాంప్ చేయబడాంది. అతన్ తన కోసాం లావాదేవీని తనిఖీ చేయలేడు, కానీ ద్వనిని చెయిన్ లప ఒక్ ప్రదేశానికి లాంక్ చేయడాం ద్వారా, సెట్ వర్క నోడ ద్వనిని ఆమోదాంచినటుల చూడగలడు మరియయ సెట్ వర్క ద్వనిని ఆమోదాంచినటుల నిరాధ రాంచిన తరాాత జోడాంచిన బాల క్ లు వసా యి.

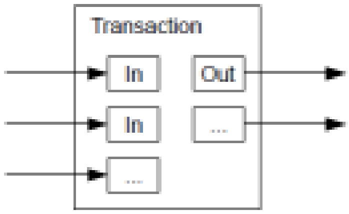


ాంద్వలల, నిజాయితీ గల నోడ లు సెట్ వర్క ని నియాంతిరస్ు సాంత వర్క్ు ధృవీక్ణ నమమదగినది అయి ఉాంటాంది. అయితే సెట్ వర్క పై ద్వడి చేసే వార్చ అధిక్ాంగా ఉాంటే అది మరాంత హానికిలస్ ాంది. సెట్ వర్క నోడ లు తమ కోసాం లావాదేవీలన్ ధృవీక్రాంచ్కోగలిగినప్టికీ, ద్వడి చేసే వాకి సెట్ వర్క న్ అధిగమిాంచడవనీ క నసాగిాంచగలిగినాంత వర్క్ు ద్వడి చేసే వాకి యొక్క క్లిత లావాదేవీల ద్వారా సరళ్క్ృత ప్దధతిని మోసాం చేయవచ్ు. చెలలని బాల క్ న్ గయరాంచినప్ుడు సెట్ వర్క నోడ ల న్ాండి హెచురిక్లన్ ఆమోదాంచడాం దీని న్ాండి ర్క్ాంచడవనికి ఒక్ వూాహాం, ప్ారి బాల క్ న్ డౌన్ లపడ చేయమని వినియోగదవ్రు సాఫ్ట వేర్ న్ పేరరనపిస్ ాంది మరియయ అసిరతన్ నిరాధ రాంచడవనికి లావాదేవీలన్ అప్రమతాం చేస్ ాంది. తర్చు చెల్లాంప్ులన్ సీాక్రాంచే వాాపారాలు మరాంత సాతాంతర భద్రత మరియయ శీఘర ధృవీక్ణ కోసాం వారి సాంత నోడ లన్ అమలు చేయాలన్కోవచ్ు.

9. విలువను కలపడం మరియు విభజంచడం

వాకిగతాంగా నవణేలన్ హాాండిల్ చేయడాం సాధామ నైనప్టికీ, టార న్ ఫర్ లప ప్రతి సెాంటుక్ు ప్రతేాక్ లావాదేవీని నిరాహ ాంచడాం క్ుదర్ని ప్ని. విలువన్ విభజాంచడవనికి మరియయ క్లపడవనికి అన్మతిాంచడవనికి, లావాదేవీలు బహుళ్ ఇన్ ప్ుట్ లు మరియయ అవుట్ ప్ుట్ లన్ క్లి ఉాంటాయి. సాధవర్ణాంగా పెదద మయన్పిటి లావాదేవీ న్ాండి ఒకన ఇన్ ప్ుట్ లేద్వ

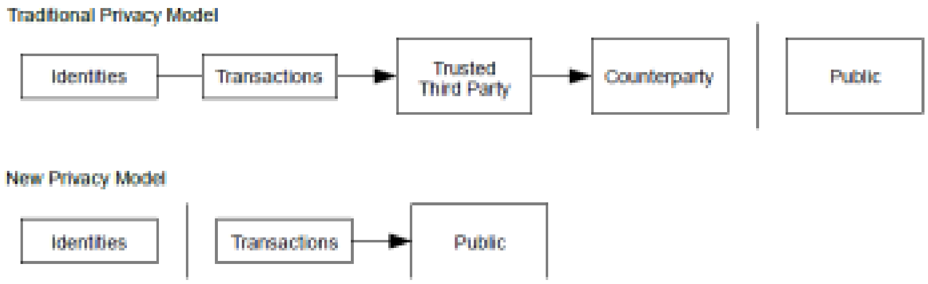
చినే మొతవి లన్ క్ల్పి బహుళ్ ఇన్ ప్ుట్ లు మరియయ గరిషరాంగా రొండు అవుట్ ప్ుట్ లు ఉాంటాయి: ఒక్టి చెల్లాంప్ు కోసాం మరియయ మరొక్టి మార్చున్ ప్ాంపినవారికి తిరిగి ప్ాంప్ుత ాంద్ి.



ఫ్ాన్-అవుట్, ఒక్ లావాద్ేవీ అనేక్ లావాద్ేవీలపై ఆధవర్పి ఉాంటూాంద్ి మరియయ ఆ లావాద్ేవీలు మరెనో వాటిపై ఆధవర్పిఉాంటాయి. ఇక్కడవ సమసా లేద్. లావాద్ేవీ చరితరయొక్క ప్ూరిసాతాంతరకాపీని సాంగరహ ాంచవలసిన అవసరాం లేద్.

10. గోపయత లేదా ప్రైవస్ీ

సాంప్రద్వయ బాాంకింగ్ మోడల్ తాంద్లప ఉనే అనీ పారటరలక్ు మరియయ ధర్ర పారటరకి కావాల్ిన్న సమాచవరానీ తాంద్ాించడాం ద్వారా సీకెరసీని మ యాంట ైన్ చేస్ి ాంద్ి. అనీ లావాద్ేవీలన్ ప్బిలక్ గా ప్రక్టాించవల్ిన్న అవసరానికి ఇద్ి విభినేంగా ఉాంటూాంద్ి. అయితే మరొక్ సిలాంలప సమాచవర్ ప్రవాహ్యానీ విచినేం చేయడాం ద్వారా గోప్ాతన్ ఇప్ుటికీ నిార్హ ాంచవచ్ు: ప్బిల క్ కీలన్ అనవమక్ాంగా ఉాంచడాం ద్వారా, ఎవరైనవ డబయబన్ వేరొక్రికి ప్ాంప్ుత నేటుల ప్బిల క్ చూడగలర్చ. కానీ లావాద్ేవీని ఎవరికీ ల్ాంక్ చేసే సమాచవార్ం లేక్ాండవ. ఇద్ి సార క్ ఎకన్చాంజీల ద్వారా విడుదల చేయబడిన సమాచవార్ం యొక్క సా యికి సమానాంగా ఉాంటూాంద్ి, ఇక్కడ వాకిగత లావాద్ేవీల సమయాం మరియయ ప్రిమాణాం "టేప్" ప్బిల క్ గా చేయబడుత ాంద్ి, కానీ పారటరలు ఎవరో చెపాాంద్కు ఇక్కడ అవకాశాం ఉాండద్.



వీటితోపాటు అదనప్◌ు ఫైర్ వాల్ గా, సాధవర్ణ యజమానికి ల్◌ాంక్ చేయబడక్◌ాండవ ప్రతి లావాద్◌ేవీకి క తి కీ జతని ఉప్యోగొంచవల్. బహుళ్-ఇన్ ప్◌ుట్ లావాద్◌ేవీలతో క నీ ల్◌ాంకింగ్ ఇప్◌ుటికీ అనివా◌ారం, ఇద్◌ి వారి ఇన్ ప్◌ుట్ లు ఒకన యజమాని సొంతాం అని తప్◌ునిసరిగా వెలలడిస్◌ి ◌ాంద్◌ి. ప్రమాదాం ఏమిటాంటే, ఒక కీ యజమానిని బహ ◌ుర్తాం చేసినటలయితే, ల్◌ాంక్ చేయడాం ద్వారా అద్◌ే యజమానికి చెంద్◌ిన ఇతర్ లావాద్◌ేవీలన్ బహ ◌ుర్తాం చేయవచ్◌ు.

11. లెక్లు

హ్యనెస్టర చెయిన్ క్◌ాంటే వేగాంగా ఆలరర్ నేట్ చెయిన్ న్ ◌ుార్పొంద్◌ిాంచడవనికి ద్వడి చేసే వాకి యొక్క దృష్◌ార ◌ాంతవనీ మేమయ ప్రిశీల్సి మయ. ఇద్◌ి నెర్వేరినప్◌ుటికీ, గాల్ న్◌ాండి విలువన్ సృషిరాంచడాం లేద్వ ద్వడి చేసే వాకికి చెందని డబయట తీస్కోవడాం వాంటి ఏక్పక మార్పులక్◌ు ఇద్◌ి వావసిన్ తెర్వద్. నోడ లు చెలలని లావాద్◌ేవీని చెల్లాంప్◌ుగా తాంగటక్రొంచవు మరియయ నిజాయితీ గల నోడ లు వాటిని క్లి ఉసే బాల క ని ఎప్◌ుటికీ తాంగటక్రొంచవు. ద్వడి చేసే వాకి అతన్ ఇటీవల ఖర్పు చేసిన డబయటన్ తిరిగి తీస్కోవడవనికి తన సొంత లావాద్◌ేవీలలప ఒక్కనీ మా◌ుర్డవనికి మాతరమే ప్రయతాంచవచ్◌ు.

హ్యనెస్టర చెయిన్ మరియయ ద్వడి అటాక్ర చెయిన్ మధా రనస్ని బినోమిల్ రాండమ్ వాక గా చెప్◌ువచ్◌ు. సకేస్ట ఈవెంట్ అనేద్◌ి హ్యనెస్టర చెయిన్ న్ ఒక బాల క తో విసిరాంచడాం, ద్వని ఆధికానీ +1 ద్వారా పెాంచడాం మరియయ వైఫలా సొంఘటన అనేద్◌ి అటాక్ర చెయిన్ న్ ఒక బాల క తో విసిరాంచడాం, తద్వారా తాంతరానీ -1 తగొంచడాం.

ఇచిన లపటు న్◌ాండి ద్వడి చేసే వాకి యొక్క సొంభావాత గ్◌ాంబల◌ర్ ◌ుార్యిన్ సమసాక్◌ు సమానాంగా ఉాంటాంద్◌ి. అప్రిమిత కెరడిట్ తో గ్◌ాంబలర్ లపటుతో పార ◌ార౦భ్మ ◌ై, బరరక్ ఈవెన్ న్ చేర్చకోవడవనికి ప్రయతాంచడవనికి అనాంతమ ◌ైన టరయల్◌్ న్ ఆడతవడన్క◌ాంద్వాం. అతన్ ఎప్◌ుడైనవ బరరక్ ఈవెన్ క్◌ు చేర్చక్◌ునే సొంభావాతన్ లేద్వ ద్వడి చేసే వాకి నిజాయితీ గల చైన్ న్ ఈ కిరాంద్◌ి విధాంగా ప్టుర క్◌ునే సొంభావాతన్ మనాం ల కికాంచవచ్◌ు [8]:

p = సొంభావాత హ్యనెస్టర నోడ తరాతి బాల క న్ గయరిస్◌ి ◌ాంద్◌ి

p = probability an honest node finds the next block
q = probability the attacker finds the next block
q_z = probability the attacker will ever catch up from z blocks behind

$$q_z = \begin{cases} 1 & \text{if } p \le q \\ (q/p)^z & \text{if } p > q \end{cases}$$

అని మా ఊహన్ బటిర, ద్వడి చేసే వాకి యొక్క బాల క్ ల సాంఖా పెరిగన క ద్ీద పార బబిల్టీ ప్డిపో త ాంద్ి. అతనికి ఎద్రృగా ఉనే అసమానతలతో, అతన్ పార ారంభ్ాంలపనే ఎద్రొకనక్పో తే, అతన్ మరొంత వెన్కృడిపో వడాంతో అతని అవకాశ్ాలు చవలా తక్ుకవగా మార్తవయి.

ప్ాంపినవార్చ లావాద్ేవీని మార్ుర్లేర్ని నిరాధ రొంచ్కోవడవనికి మయాంద్ క తి లావాద్ేవీని సీక్రొంచే వాకి పొంతకాలాం వేచి ఊండవలప మేమయ ఇప్ుడు ప్రిశీల్సా మయ. ప్ాంపిన వాకి ద్వడి చేసే వాకి అని మేమయ ఊహ సా మయ, అతన్ గరహీత తనక్ు క ొంత కాలాం చెల్లాంచవడని నమిమ, క ొంత సమయాం గడిచిన తరాాత తనకన తిరిగి చెల్లాంచడవనికి ద్వనీ మార్చుకోవాల్. అద్ి జరిగినప్ుడు రిసీవర్ అప్రమతాం చేయబడుత ాంద్ి, కానీ ప్ాంపినవార్చ చవలా ఆలసాం అవుత ాందని ఆశస్ి నవేర్చ.

రిసీవర్ క తి కీ జతని ఉతుతి చేస్ి ాంద్ి మరియయ సాంతక్ాం చేయడవనికి క ద్ిదసేప్టి మయాంద్ ప్ాంపినవారికి ప్పిల క్ కీని ఇస్ి ాంద్ి. ఇద్ి ప్ాంపినవార్చ మరొంత మయాంద్క్ు వెళ్లల వర్క్ు నిార్ంతార్ం ప్ని చేయడాం ద్వారా బాల క్ుల గొలుస్ను సిదధాం చేయక్ాండవ నిరోధిస్ి ాంద్ి, ఆ సమయాంలప లావాద్ేవీని అమలు చేస్ి ాంద్ి. లావాద్ేవీని ప్ాంపిన తరాాత, నిజాయితీ లేని ప్ాంపిన వాకి తన లావాద్ేవీ యొక్క ప్రతవామేయ సాంసకర్ణన్ క్లి ఉనే సమాాంతర్ గొలుస్పై ర్హసాంగా ప్ని చేయడాం పార ార్ంభిసా డు.

లావాద్ేవీ బాల క్ కి జోడించబడే వర్క్ు సీక్ర్ి వేచి ఊంటాడు మరియయ ద్వని తరాాత z బాల క్ లు ల్ాంక్ చేయబడతవయి. ద్వడి చేసే వాకి సాధిాంచిన ప్ురోగతి యొక్క ఖచిితమ ైన మొతాం అతనికి తెల్యద్, అయితే నిజాయితీ గల బాల క్ లు ఒకోక బాల క్ క్ు సగటున ఆశాంచిన సమయానీ తీస్క్ునవేయని ఊహ సి, ద్వడి చేసేవారి సాంభావా ప్ురోగతి ఆశాంచిన విలువతో పాయిసన్ ప్ాంపిణీ అవుత ాంద్ి:

$$\lambda = z\frac{q}{p}$$

To get the probability the attacker could still catch up now, we multiply the Poisson density for each amount of progress he could have made by the probability he could catch up from that point:

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \left\{ \begin{array}{ll} (q/p)^{(z-k)} & \text{if } k \le z \\ 1 & \text{if } k > z \end{array} \right\}$$

Rearranging to avoid summing the infinite tail of the distribution...

$$1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \left(1 - (q/p)^{(z-k)}\right)$$

Converting to C code...

```
#include <math.h>
double AttackerSuccessProbability(double q, int z)
{
    double p = 1.0 - q;
    double lambda = z * (q / p);
    double sum = 1.0;
    int i, k;
    for (k = 0; k <= z; k++)
    {
        double poisson = exp(-lambda);
        for (i = 1; i <= k; i++)
            poisson *= lambda / i;
        sum -= poisson * (1 - pow(q / p, z - k));
    }
    return sum;
}
```

Running some results, we can see the probability drop off exponentially with z.

```
q=0.1
z=0    P=1.0000000
z=1    P=0.2045873
z=2    P=0.0509779
z=3    P=0.0131722
z=4    P=0.0034552
z=5    P=0.0009137
z=6    P=0.0002428
z=7    P=0.0000647
z=8    P=0.0000173
z=9    P=0.0000046
z=10   P=0.0000012

q=0.3
z=0    P=1.0000000
z=5    P=0.1773523
z=10   P=0.0416605
z=15   P=0.0101008
z=20   P=0.0024804
z=25   P=0.0006132
z=30   P=0.0001522
z=35   P=0.0000379
z=40   P=0.0000095
z=45   P=0.0000024
z=50   P=0.0000006
```

Solving for P less than 0.1%...

```
P < 0.001
q=0.10   z=5
q=0.15   z=8
q=0.20   z=11
q=0.25   z=15
q=0.30   z=24
q=0.35   z=41
q=0.40   z=89
q=0.45   z=340
```

12. ముగింపు

విశాసనీయత కోసాం ఎద్రుచూడక్ాండవ ఎలకారా నిక్ లావాద్ేవీల వావసిన్ మేమయ ప్రతిపాద్ిాంచవమయ. మేమయ డిజిటల్ సాంతకాలతో తయార్చ చేయబడిన కాయిన్్ యొక్క సాధవర్ణ ఫేరమ్ వర్క తో మా ప్నిని పార ార్ంభిాంచవమయ. ఇద్ి యాజమానాంపై బలమ ైన నియాంతరణన్ తాంద్ిస్ి ాంద్ికానీ డబయల్ ఖర్చున్ నిరోధిాంచే మా్ార్ం లేక్ాండవ అసాంప్ూర్ణాంగా ఉాంద్ి. ద్ీని ప్రిషకరిాంచడవనికి, నిజాయితీ గల నోడ లు మ జారిటీ సీపీయయ శకిని నియాంతిరాంచవల్. అప్ుడు ద్వడి చేసే వాకికి లావాద్ేవీల ప్ైల క్ హ సరరటని రికా్ర్ చేయడవనికి ప్ూా ఫ్-ఆఫ్-వర్క ఉప్యోగిాంచి పీర్-టు-పీర్ నెట్ వర్క న్ మేమయ ప్రతిపాద్ిాంచవమయ. నెట్ వర్క ద్వని నిరామణవతమక్మ ైన సర్ళలప బలాంగా ఉాంద్ి. నోడ్ చినే సమనాయాంతో ఒకనసారి ప్ని చేసా యి. వాటిని గయరిాంచవల్ిన అవస్ార్ం లేద్, పాంద్కాంటే సాంద్ేశ్ాలు ఏద్ైనవ నిరిదషర ప్రద్ేశ్ానికి మళ్లాంచబడవు మరియయ ఉతిమ ప్రయతేం ఆధవ్ార్ంగా మాతరమే ప్ాంపిణీ చేయాల్. నోడ లు తమ ఇష్ార న్ాార్ంగా నెట్ వర్క న్ విడిచిపెటిర, తిరిగి చేర్వచ్ు, వార్చ పో యినప్ుడు ఏమి జరిగిాందనే ద్వనికి ర్చజువుగా ప్ని చేసే గొలుస్న

తాంగటక్రొంచవచ్ు. వార్చ తమ

సీపీయయ శకితో ఓటు వేసా ర్చ, చెలుల బాటు అయా బాల క్ లన్ వొ డిగొంచడాం ద్వారా మరియయ చెలలని బాల క్ లపై ప్ని చేయడవనికి నిరాక్రొంచడాం ద్వారా వాటిని తిర్సకరొంచడాం ద్వారా వారి తాంగటకారానీ తెల్యజనసా ర్చ. ఈ ఏకాభిపార య విధవనాంతో ఏవైనవ అవసర్మ ైన నియమాలు మరియయ వోర తవ్వకాలు అమలు చేయబడతవయి.

References

[1] W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.

[2] H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In *20th Symposium on Information Theory in the Benelux*, May 1999.

[3] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In *Journal of Cryptology*, vol 3, no 2, pages 99-111, 1991.

[4] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," In *Sequences II: Methods in Communication, Security and Computer Science*, pages 329-334, 1993.

[5] S. Haber, W.S. Stornetta, "Secure names for bit-strings," In *Proceedings of the 4th ACM Conference on Computer and Communications Security*, pages 28-35, April 1997.

[6] A. Back, "Hashcash - a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf, 2002.

[7] R.C. Merkle, "Protocols for public key cryptosystems," In *Proc. 1980 Symposium on Security and Privacy*, IEEE Computer Society, pages 122-133, April 1980.

[8] W. Feller, "An introduction to probability theory and its applications," 1957.

రిఫరెన్సులు

[1] W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.

[2] H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimaltrust requirements," In 20th Symposium on Information Theory in the Benelux, May 1999.

[3] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In Journal of Cryptology, vol 3, no2, pages 99-111, 1991.

[4] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time stamping,"In Sequences II: Methods in Communication, Security and Computer Science, pages 329-334, 1993.

[5] S. Haber, W.S. Stornetta, "Secure names for bit-strings," In Proceedings of the 4th ACM Conferenceon Computer and Communications Security, pages 28-35, April 1997.

[6] A. Back, "Hashcash - a denial of service counter
measure,"
http://www.hashcash.org/papers/hashcash.pdf, 2002.

[7] R.C. Merkle, "Protocols for public key cryptosystems," In Proc. 1980 Symposium on Security andPrivacy, IEEE Computer Society, pages 122-133, April 1980.

[8] W. Feller, "An introduction to probability theory and its applications," 1957.